The Impact of Culture and Religion on Digital Forensics: The Study of the Role of Digital Evidence in the Legal Process in Saudi Arabia

Najah Abdulaziz Alfaize, BA, Msc

THESIS SUBMITTED TO FULFILL THE REQUIREMENTS FOR THE AWARD OF

DOCTOR OF PHILOSOPHY

FACULTY SOFTWARE TECHNOLOGY RESEARCH LABORATORY (STRL)
DE MONTFORT UNIVERSITY

LEICESTER, UK

2015

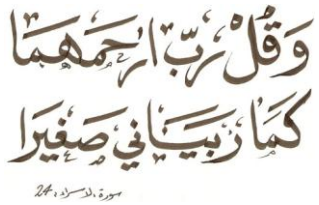
Declaration

I, Najah Alfaize (P08040154), declare this thesis is entirely myself work unless otherwise stated, referenced or acknowledged. I confirm this document submitted for the award of doctor of philosophy (PhD), in the faculty software technology research laboratory (STRL), De Montfort University Leicester, UK. Also, I confirm it has not been submitted for any qualifications at any other institutes.

Signature: …… Date: ……

DEDICATED TO

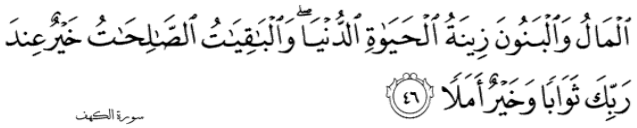
My beloved mother and father



“And lower unto them the wing of submission through mercy, and say: My Lord! Have mercy on them both as they did care for me when I was little.” (Quran17:24)

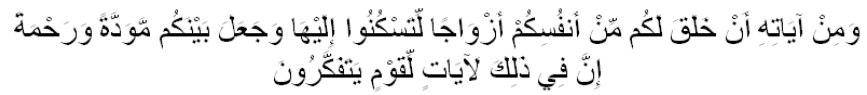
My five sweet sons

“Wealth and sons are allurements of the life of this world” (Quran: 46)



My Husband

And among His Signs is this, that He created for you mates from among yourselves, that ye may dwell in tranquillity with them, and He has put love and mercy between your (hearts): verily in that are Signs for those who reflect (Quran, 30:21).



Acknowledgment

First and foremost, I wish to express my great thanks to my supervisor Professor Duska Rosenberg for her precious guidance and support during my study. I highly appreciated her suggestions and supports all the way in the course of this thesis. I am also thankful to her for her care, ideas and encouragement which without it I would not have completed this thesis.

I would like to thank Saudi Cultural bureau, Saudi Arabia Embassy in London for the Generosity and support I received during my PhD study.

Also, I wish to thanks Professor Hussein Zedan for his support, and guidance at the early stages of this research.

I will never forget the great the supports and valuable guidance I had from all the staff at the faculty software technology research laboratory.Thank you very much.

Finally, I would like to thank my brothers and sisters for their supports which helped me to completing this Ph.D even though they are far away from me most of the time.

Abstract

This work contributes to the multi-disciplinary community of researchers in computer science, information technology and computer forensics working together with legal enforcement professionals involved in digital forensic investigations. It is focused on the relationship between scientific approaches underpinning digital forensics and the Islamic law underpinning legal enforcement. Saudi Arabia (KSA) is studied as an example of an Islamic country that has adopted international guidelines, such as ACPO, in its legal enforcement procedures. The relationship between Islamic law and scientific ACPO guidelines is examined in detail through the practices of digital forensic practitioners in the process of discovery, preparation and presentation of digital evidence for use in Islamic courts in KSA.

In this context, the influence of religion and culture on the role and status of digital evidence throughout the entire legal process has been the main focus of this research. Similar studies in the literature confirm that culture and religion are significant factors in the relationship between law, legal enforcement procedure and digital evidence. Islamic societies, however, have not been extensively studied from this perspective, and this study aims to address issues that arise at both professional and personal levels. Therefore the research questions that this study aims to answer are: in what way and to what extent Islamic religion and Saudi culture affect the status of digital evidence in the KSA legal process and what principles the practitioners have to observe in the way they treat digital evidence in judicial proceedings.

The methodology is based on a mixed-method approach where the pilot questionnaire identified legal professionals who come into contact with digital evidence, their educational and professional profiles. Qualitative methods included case studies, interviews and documentary evidence to discover how their beliefs and attitudes influence their trust in digital evidence. The findings show that a KSA judge would trust witnesses more than digital evidence, due to the influence of tradition, which regards justice and law

to arise from the relationship between Man and God. Digital evidence, as it arises from the scientific method, is acceptable, but there is underlying lack of trust in its authenticity, reliability and credibility. In the eyes of the legal enforcement professionals working in all areas of the KSA legal process, acceptance of digital evidence in the KSA judicial system can best be improved if knowledge, education and skills of digital forensics specialists is improved also, so that they can be trusted as expert witnesses. This further shows the significance of KSA laws, regulations and education of digital forensic experts as the primary means for establishing trust in digital evidence. Further research following from this study will be focused on comparative studies of other Islamic non-Islamic legal systems as they adopt and adapt western guidelines such as ACPO to their religion, culture and legal systems

TABLE OF CONTENTS

GLOSSARY OF ABBREVIATIONS AND ACRONYMS

ACPO	Association of Chief Police Officers
ATM	Automatic Teller Machine
BIPP	The Bureau of Investigation and Public Prosecution
BSA	British Standards Institute
CITC	Communications and Information Technology Commission
DFRWS	Digital Forensic Research Workshop
DNA	Deoxyribonucleic Acid
DOJ	Department of Justice
ICT	Information and Communications Technology
IOCE	International Organization on Computer Evidence
IODE	International Organization on Digital Evidence
IP	Internet Protocol
IS	Information System
IT	Information Technology
KSA	Kingdom of Saudi Arabia
LE	Legal Enforcement
MOC	Ministry of Commerce

NIJ	National Institute of Justice
PDAS	Personal Data Assistants
SAMA	Saudi Arabian Monetary Agency
SLA	Service Level Agreement
SMS	Short Message Service (Text Message)
SOPs	Stander Operating Procedures
TCP	Transmission Control Protocol
UK	United Kingdom
US	United States
ACPO	Association of Chief Police Officers

LIST OF TABLE

Chapter One

Introduction

1.1 Background and motivation

According to the ACPO, 'cybercrime' involves the, "…use of a network, Internet technology or computer to commit or facilitate the commission of crime" (ACPO, 2011). While, the Bureau of the Expert Group on Cybercrime (BEGC, 2013) proposes 14 acts that may constitute cybercrime, classified into three broad groups;

1. Acts against the confidentiality, integrity and availability of computer data or systems
2. Computer-related acts for personal or financial gain or harm
3. Computer content-related acts

Therefore, cybercrime in a broader sense (computer-related crimes) covers any illegal behaviour dedicated by, or in relation to, a digital system or network; such as illegal ownership and offering or distributing information by means of a computer system or network (Williams K, 2004). Cybercrime and digital security are hardly to be separated in a consistent environment. The United Nations General Assembly's (2010) declaration on digital security addresses cybercrime as one major challenge (Gercke M, 2012).

Accordingly, digital evidence comes from different sources, such as computer, laptops, cameras, mobile phones, music players, PDAs, network servers (e.g., supporting applications such as Web sites, e-mail, and social networks); and network hardware (e.g. routers) (Brown, 2010; Casey, 2011). These digital devices store enormous volume of data and information about our daily life (O'Harrow, 2006). Ball (2008), Casey (2011), Kerr (2005), stated that digital evidence is growing in quantity and weight in criminal litigation where the Judges should make a decision what evidence would be taken and need to assess the probative weight alongside with the pre-judicial effect of any evidence that is obtainable (Cohen, 2010). Therefore, it could be quite difficult for untrained professional to apply critical analysis and give accurate reports on digital evidence to be offered as fact in a courtroom (Mason, 2008).

Digital devices hold huge amounts of evidence that is worth investigating, but can

be quite hard to handle. The volumes of data stored in the devices increases with time as some of them can store terabytes of data (BEGC, 2013). However, very few items in this huge mixture might be really relevant to a crime case (BEGC, 2013). These features create difficulties in extracting, correlating and translating practical and significant portions of data and information that may be necessary for improving the understanding, interpretation and resolution of a case. Consequently, digital evidence (DE) requires uniform and proven methods for searching, handling, validating and analysing data (BEGC, 2013).

The volumes of data stored in the devices increase with time as some of them are capable of storing terabytes of data. However, very few pieces of data from this huge mixture are really relevant to a case. These features create difficulties in extracting, correlating and translating practical and significant portions of data and the information which may be necessary for improving the understanding, interpretation and resolution of a case (Saleem, 2015). Consequently, digital evidence requires uniform and verified methods for searching, handling, validating and analysing it. These methods must protect the integrity and authenticity of the digital evidence. Such well validated and well-tested methods surely will help to obtain related and weighty digital evidence and thus increase the chances of its admissibility (Casey, 2011).

One common feature all authors stated; the eventual goal of digital forensics is to provide lawful and accurate digital evidence in a courtroom rather than just test digital devices or examining the digital data (Saleem, 2015). Consequently, most Western countries follow firm procedures, such as the Association of Chief Police Officers (ACPO) in UK and National Institute of Justice (NIJ) in the USA, in order to present legally sound digital evidence in a courtroom.

1.2 Problem specification

The literature shows that crimes in general are vary from society to society depending on cultures and religion, for example Slander and Pornography have different concept in different cultures. In Islamic societies any sort female body exposure would be consider as

pornography. As well, slander, gambling, and abusing religionist-scholars are prohibited while it could be acceptable behavior in some other societies as personal freedom (Ge Zhu, 2010), Slay and Quirchmayr (2004). With different religion and cultural backgrounds are likely to act or to respond to an event differently (Greenfield, 1997). This view is also supported by Wertsch et al. (1995), who acknowledge that culture and society are two major factors which influence cognitive development. Also, Solano-Flores and Nelson-Barber (2001) make a similar statement that, "The conceptual relevance of cultural validity is supported by evidence that culture and society shape an individual's mind and thinking". Lastly, Greenfield (1997) notes that the way an individual constructs knowledge and creates meaning from experience is affected by culture. On the other hand, On the other hand, Religion influences different cultures in various ways, and it would impact on the culture in various ways at different times. When individuals within a culture believe in a specific religion strongly, the religion will have enormous influence on their culture, where, the culture will accept only those behaviours and ways of thinking that are acceptable to their religion (Aldashev G, 2014).

According to Joseph Schacht "Law is still the most important component in the struggle which is being fought in Islam between traditionalism and modernism under the impact of Western Ideas". However, the theory of law on Islam differs from the western theory of law significantly; the philosophy of Islam says; "this world was created by only one God known and all materials on the planet and in the universe were created by Him and He alone managed this creation" (Hassan, 1994). The Islamic religion is built on the relationship between an individual and God, which is moral, ethical and obliges a person to tell the truth in a court of law. Consequently, there is a conflict between the scientific and impersonal nature of the western legal system that is generated through scientific evidence, and the moral and religious obligation that is based on faith and trust of the Islamic religion.

The methods of proving offences in Islamic law are a controversial issue because there are two points of view (AlKarmi 2005; Al-Zohaili 1994). The first point of view believes that these methods are limited to only classical methods such as witnesses,

confession and oath. These views are based on the Quran and the Sunnah (Al-Zohaili 1994). The second point of view believes that these methods are unlimited to include any method that leads to the truth such as witness, confession, substantial evidence, bearing testimony (Al Qarinah) and a scientific method (Al-Zohaili 1994).

However, the Islamic societies have not been extensively studied. In this study these impacts of religion and culture rare investigated in relation to the role and status of digital evidence in the entire legal process in Saudi Arabia (as an example of Islamic law). Therefore, the research questions that this study aims to answer are: in what way and to what extent do Islamic religion and Saudi culture affect the status of digital evidence in the legal process? What principles do the practitioners have to observe in the way they treat digital evidence in the judicial proceedings?

1.3 Summary of related existing research

Slay and Kearney (2000) that concludes that the Chinese education system is different from the Western education system because the Chinese have a teaching attitude which is different from the Western teaching philosophy. Also confirms that the Chinese worldview is based on Confucianism since it is the primary educational trend. The main concept of Confucianism concentrates on the relationship between man, nature, and the heavens, rather than focusing on the value of science as defined in a Western worldview (Lin, 2008). Also, Slay (2000) shows that culture and gender are two factors which affect students' attitudes to computers and learning. In other words, this is to say that culture is undeniably a feature that affects science applications.

While, Lin's (2008) directly compares the Australian and Taiwanese cultures as they apply to the field of computer forensics. Lin proved there were clear differences between the two different cultures based on his findings. He introduced the Hofstede phenomena: the first being that culture is not universal and that cultural difference are nationally based, using 'national culture', to describe that each nation has its unique

culture. The second phenomenon is that an individual's behaviour is indeed affected by his or her unique culture. Lin also introduced the five dimensions (Current Situation Dimension, Policy and Organization Dimension, Education Dimension, Law Dimension, and Personal Preference and Skill Dimension) he used to describe the latest computer forensic situations and to compare the differences between cultures in Australia and Taiwan (Lin's thesis, 2008). Where he concludes that in both countries where Australian common law and Taiwanese laws are designed, there are two very different perspectives on various societal foundations. The differences are so extreme that these cannot be easily mapped, as there are many stages and processes in each that the other lacks. The cultural principles behind the responses from the two countries are based on different societal precepts.

Moreover, Leidner (2006) reviewed 51 articles which examine cross-cultural studies of Information Technology and came up with the following six themes. These themes clearly show how different types of firm-wide and culture values have an impact on information systems development, adoption, diffusion, use, outcomes, management and strategy. On the other hand, Lin's study concludes that in both countries where Australian common law and Taiwanese laws are designed, there are two very different perspectives on various societal foundations. The differences are so extreme that these cannot be easily mapped, as there are many stages and processes in each that the other lacks. The cultural principles behind the responses from the two countries are based on different societal precepts. These works are powerful illustrations of the relationship between culture and different sciences.

Furthermore, Maghaireh (2009) surveys and analyses laws passed to address different digital evidence admissibility in a courtroom between Jordan, Australia and USA. Also, he examines the judiciary's role in admitting the digital evidence. He shows that Jordanian laws express the inadequacies which need to be addressed if legislation is to achieve its objective of admitting the digital evidence. The inadequacies are both legislative and non-legislative, in both technology and litigation support, and also education and training. From a legal point of view, digital evidence admissibility is

scattered over a broad range of statutes which lack uniformity and comprehensiveness. Jordanian laws (the Electronic Transactions Law and Evidence Law) require completeness as they demonstrate an incomplete understanding of digital evidence. The Electronic Transactions Law only admits electronic contracts and messages that are generated, sent, received or stored electronically. Meanwhile, the Evidence Law only reveals e-mails and other computer stored evidence. As a result, many types of computer generated evidence, such as log files, metadata, and hash value is beyond the ambit of the Electronic Transactions Law 2001 or the Evidence Law because they are neither electronic contracts, nor messages in the meaning of the Electronic Transactions Law (Maghaireh, 2009).

1.4 Evaluation methods

The focus of the analytical framework developed in this study is on the role and status of digital evidence in the Saudi Arabian legal practice in comparison with the traditional evidence. The use of digital evidence is new, requires a considerable degree of expertise in the fields of computer science, information technology, as well as familiarity with legal regulations and constraints. The nature of digital evidence is that is it non-intuitive, precise and every action can be traced and proved scientifically. For these reasons the value of digital evidence is different from the value of human witnesses. It is indeed, more difficult for the legal professionals (not trained in technology) to establish beyond any doubt that particular digital evidence is authentic and reliable, than to trust their own judgment based on legal education and experience.

Therefore, it is important to follow the path of digital evidence from its discovery to the end of the legal process when innocence or quilt is established and sentences pronounced. It is also important to examine how digital evidence is treated throughout the entire legal process that is, in what way it is collected and analysed, presented to the court and regarded by the judges as a reliable proof of guilt or innocence of the defendants. A broad approach to engage all stakeholders involved is important in addressing the research question – that is - in what way and to what extent the Islamic religion and Saudi Arabian

culture affect the status of digital evidence in the legal process. Therefore the focus of this study is to, examine the principles practitioners have to observe in the way they treat digital evidence in the judicial proceedings, especially how Islamic laws stand in respect to the admissibility of various kinds of digital data as evidence and how digital forensic practitioners follow this in practice. Saudi Arabia is an example of an Islamic country practicing Islamic law and it is expected that the findings of the study in Saudi Arabia can be generalized to other Islamic societies.

According to Mingers (2001), research results will be richer and more reliable if different research methods, preferably from different paradigms, are routinely combined. However, since qualitative method is the respectable way to gather facts about people's beliefs, feelings, experiences were used. The methodological approach is based on mixed method where qualitative questionnaires were used in the pilot study to identify the legal professionals who come into contact with digital evidence, their educational and professional profiles. While, case interview methods were used in the in-depth study of their day-to-day work. Since qualitative research normally does not have numerical data or statistic information to prove and to support the accuracy of its findings, a variety of methods were needed to ensure the reliability and robustness of the research approach developed in this study. Four main methods were used; historical (literature) review, questionnaire survey, case study and legal case reports. These methods follow the concept of the triangulation to improve the reliability of the results and to prove the credibility of the findings of this research.

1.5 Thesis roadmap

Chapter One: Gives an introduction to the thesis

Chapter Two: entitled "The relationship between culture, religion/law and science" the aim of this chapter is to support the argument that different cultures and religions have different impacts on the way they regard science and its application in the daily lives of the members of any particular culture. Religion and culture can affect digital forensic practitioners in the way they observe and treat digital evidence in the legal process. Section

one examines the effects of religion and culture on science and its applications, the relationship between culture and education, and the study of information systems, digital forensics and digital evidence. Furthermore, discuss the relationship between culture and religion and the role of digital forensics in Saudi Arabia's legal system as an example of an Islamic country where digital forensics provides a relatively new input in the legal process.

Chapter 3: entitled "Digital forensics and digital evidence" the objective of this chapter is to examine the role, status validity, integrity and the admissibility of digital evidence in western law. It demonstrates the particular characteristic features and inherent risks associated with digital evidence from both technical and legal perspectives. The nature and characteristics of digital evidence will be examined for their effects on evidence admissibility. The chapter then evaluates the relationship between procedures and guidelines in the UK (ACPO), USA (NIJ) and the procedures and guidelines that are needed for Saudi Arabia, (since they do not yet exist), which would take into account the specifics of Islamic law. This chapter serves to identify what the practitioners have to observe the way they treat digital evidence in the legal process, and how culture and religion factors could influence the status of digital evidence. Lastly, to what extent are judges likely to recognize different kinds of digital evidence in developed countries?

Chapter four: Digital evidence in Islamic law, this chapter aims to examine the Islamic law; in what way and to what extent does Islamic religion affect the status of digital evidence in the legal process? What principles do the practitioners have to observe in the way they treat digital evidence in the judicial proceedings? Also, this chapter will provide the base line to identify how digital forensic practitioners resolve this apparent conflict in practice. Also, clarifies the meaning of Islam, Shariah, and Islamic (Shariah) Law, as they have a common root but have developed individually and are quite separate today. Also, discuses the rules, principles, teachings and disciplines derived from the primary sources of Islam: the Quran and Sunnah are discussed and the legal structure governing Islamic law, communities and social norms are examined in this section. Moreover, examines the criminal procedure in Islamic law as there are different from the point view they have specific set of offences, each type of these crimes are punished by specific penalties.

CHAPTER 5: entitled "the role and status of digital evidence in SA legal practice – analytical framework and research methodology. This chapter aims to examine in what way and to what extent the Islamic religion and culture affect the status of digital evidence in the legal process from the perspectives of the legal practitioners involved in the entire process. It also examines the principles practitioners have to observe in the way they treat digital evidence in the judicial proceedings bearing in mind the differences between the traditionalist views based on religion and the digital forensic guidelines based on science. Finally, it assesses how digital forensic practitioners resolve this apparent conflict in practice. Moreover, discuss the research methodology used for this work, as a means of discovering the most powerful way of answering the research questions. This chapter not only introduces the differences between research methodologies but also gives the explanations of quality measurements, such as reliability and validity that apply to this research.

Chapter 6: **Discussion of findings this chapter** this chapter present and discusses the findings of the survey, cases interview and the legal cases. The religion and cultural explanations for these results are presented and discussed detail in this chapter. The outcomes are presented by the four dimensions these dimensions are used to analyse the data obtained by means of the mixed methods described in previous chapters as discussed in chapter five to give a better understanding of the current circumstances within digital forensics in Saudi Arabia. To understand more about legal procedure and law in Saudi Arabia, three legal cases of digital crimes are presented and discussed in this chapter too. The triangulation of the four methods were used in this thesis to presented, discussed and examine the major research questions.

Chapter 7: Conclusion, Recommendation andFuture Work, this chapter conclude and purposed anovel digital forensic guidelines enhanced with steps to provide a roadmap for Saudi Arabia (since such guidelines do not yet exist) can provide the basis for improvement in Saudi Arabia and for further similar studies in other Islamic countries. In addition, identifies areas for future works.

Chapter Two

The relationship between culture, religion/law and science

2.1 Introduction of the chapter

This thesis presents a multi-disciplinary project that combines research on the legal enforcement process (police, courts) and the use of digital evidence in the process with special emphasis on the role cultural and religious values have in this context. Therefore, the aim of this chapter is to support the argument that different cultures and religions have different impacts on the way they regard science and its application in the daily lives of the members of any particular culture. Religion and culture can affect digital forensic practitioners in the way they observe and treat digital evidence in the legal process. Religion and culture may also play a role in the legal process, with the cultural factors influencing the status of the digital evidence.

Section 2.1 examines the effects of religion and culture on science and its applications, the relationship between culture and education, and the study of information systems, digital forensics and digital evidence. First, it examines the impact of religion and culture on an individual's mind and thinking. Section 2.2 discusses related works done by Slay, Lin, Leidner, and Maghaireh, which focus on the relationships between culture and religion on science among Islamic and non-Islamic societies. This relationship is significant since it shows that applications of science are influenced by different cultures, thus, the link between religion, culture and science application is then established. These related works are powerful illustrations of the relationship between religion, culture and the sciences.

Section 2.3 focuses on the relationship between culture and religion and the role of digital forensics in Saudi Arabia's legal system as an example of an Islamic country where digital forensics provides a relatively new input in the legal process.

2.2 The Links between Culture, Law and Religion

2.2.1 Background

Several academic opinions (Wertsch et al. 1995, Greenfield 1997, and Solano-Flores and Nelson-Barber 2001) show that culture is not universal, and culture can affect an individual's mind-set and way of thinking. Also, culture changes the way a person constructs knowledge and forms experience. Furthermore, these studies confirm that culture and society are the two main factors which affect cognitive development. People with different cultural backgrounds are likely to act or to respond to an event differently (Greenfield 1997). This view is also supported by Wertsch (1985), and Wertsch et al. (1995), who acknowledge that culture and society are two major factors which influence cognitive development. Also, Solano-Flores and Nelson-Barber (2001) make a similar statement that, "The conceptual relevance of cultural validity is supported by evidence that culture and society shape an individual's mind and thinking". Lastly, Greenfield (1997) notes that the way an individual constructs knowledge and creates meaning from experience is affected by culture. On the other hand, Religion influences different cultures in various ways, and it would impact on the culture in various ways at different times. When individuals within a culture believe in a specific religion strongly, the religion will have enormous influence on their culture, where, the culture will accept only those behaviours and ways of thinking that are acceptable to their religion (Aldashev G, 2014).

2.2.2 Slay's Works

Slay has spent years researching the impact of culture in science, and her studies mainly express the idea that Australian and Taiwanese perspectives have different explanations for the conceptualizations of nature - her focus is mainly on the issue of culture and science education. Her works, therefore, are critical in building the link between culture and science as far as this study is concerned.

This is exemplified by Slay and Kearney (2000) that concludes that the Chinese education system is different from the Western education system because the Chinese have a teaching attitude which is different from the Western teaching philosophy. She also confirms that the Chinese worldview is based on Confucianism since it is the primary educational trend. The main concept of Confucianism concentrates on the relationship between man, nature, and the heavens, rather than focusing on the value of science as defined in a Western worldview (Lin, 2008). Furthermore, Confucius recognised five social associations, and they are: father and son, ruler and subject, husband and wife, elder and younger brother, and friend and friend. In Confucius's theory, the hierarchy is respected, and the relationship between a supervisor and his or her subordinate is esteemed. This theory also infers the importance of interpersonal relationships (Slay and Kearney, 2000; Lin, 2008).

Hong (1991) also explains the differences between Chinese and Western education by noting that the main concept of Chinese education is that they give more respect to the elderly and books. Moreover, the Chinese also pay more attention to authority, tradition and experience. This explains the difference between China and the West since the Chinese use their sole teaching philosophy to teach students about academic subjects, including science. Hong (1991) gives more explanation to the difference in the teaching philosophy. He notes that a Chinese person's mind may think differently from a Western person's mind, even if they face the same question. This indicates that they are likely to have different solutions and different ideas to the same question, although they both will have the same answer to the question at the end (Lin, 2008). Also, Slay (2000) show that culture and gender are two factors which affect students' attitudes to computers and learning. Similarly, Ogunniyi (1988) notes that there is difference between the African and Western worldviews. Although Western and African science deals with the same natural world, they construct different interpretations to explain it. In other words, this is to say that culture is undeniably a feature that affects science applications. Slay's works demonstrates the difference between Chinese and Western culture, since Chinese educators use Confucianism philosophy to teach students about academic subjects, including science.

In summary, her works not only indicating that Confucianism is the central philosophy control Chines culture but also demonstrates that Confucianism plays a significant role in science in Chinese traditional science.

2.2.3 Dorothy E. Leidner's Work

There is wide range of literature that has demonstrated that there is a significant relationship between Information Technology (IT) and culture. Culture has been applied to describe a wide range of social behaviours and outcomes in organisational settings (Keesing 1974; Nadler and Tushman 1988), including firm effectiveness firm performance (Gordon and Di Tomasso 1992; Kotter and Heskett 1992), corporate strategy, job attitudes (Birnbaum and Sommers 1986), administrative practices, merger and acquisition outcomes, technology transfer practices, and conflict resolution strategies in product innovation settings (Hussain 1998). Culture also has a great impact on information-related behaviours, comprising, at the basic level, what is considered to be legitimate information (Leidner D, 2006). Leidner (2006) reviewed 51 articles which examine cross-cultural studies of IT and came up with the following themes:

Theme 1: Culture and Information Systems Development (ISD)

According, Keil et al. (2000) on this theme investigate the relationship between national culture and perceptions of ISD project risk and risk management behaviours carried out matching lab experiments in Finland, Singapore, and the Netherlands to investigate how the escalation of commitment behaviour in software projects differs among cultures. They concluded that cultures low in uncertainty avoidance had lower perceptions of project risk than cultures high in uncertainty avoidance. In another study, they examined the impact of national culture on the predisposition to report bad news about failing ISD projects (Tan, Smith, and Keil, 2003). They found out that individualistic cultures (USA) were more predisposed to report bad news on troubled IT projects than collectivistic cultures.

Theme 2: Culture and Information Technology Adoption and Diffusion

In 16 studies by Png et al.'s (2001) which address the question of whether culture influences the adoption and diffusion of IT study (surveying 153 businesses across 23 countries), concluded that countries high in uncertainty avoidance are less likely to adopt

frame relay technology. Similarly, Hasan and Ditsa's (1999) interpretive study of 10 institutions in the Middle East, Africa, and Australia found out that IT is less readily adopted in risk-averse cultures. Equally, Hill et al.'s (1998) field study of five Arab countries shows the certainty of cultural values (preference for face-to-face interaction).

In relation to this, the examination of university students by Thatcher et al. (2003) shows that students from countries high in uncertainty avoidance were less willing to experiment with new information technologies. Loyalty to family, concepts of time, religion, and gender relations tended to either facilitate or impede technology transfer to the host countries. A study of internet diffusion determined that the degree of similarity in values concerning technology between using and host countries will influence the level of adoption of IT (Loch et al, 2003). In particular, they discovered that acceptability of computers (a value) in Arab countries was positively related to the level of internet usage. These conclusions provide reasonable evidence that value orientations (national, organisational, or sub-cultural) may predispose certain social groups toward either favourable or unfavourable IT adoption and diffusion behaviours (Leidner D, 2006).

Theme 3: Culture, Information Technology Use and Outcomes

Eighteen studies were incorporated and a diverse set of methodologies were used to examine the influence of culture on IT use and outcomes. This theme tries to find out whether the same IT can be used in comparable ways over cultures and will appear to have similar advantages, or will the same IT be used differently across cultures and result in different benefits (Leidner, 2006). Chau et al. (2002) found out that customer attitudes toward the Internet differ hugely between Hong Kong (value preferences for shared loyalty and relationships) and the United States (value preferences for personal competence and loyalty to oneself) subjects. As a result, people from Hong Kong used the Internet mainly for social communication, while US respondents used it principally for information research. These results suggest that cultural values shape how people use information technology. Similarly, a study on administrative information systems use among Swedish, Mexican and US managers concluded that cultural values influenced perceptions of

executive information systems (EIS) use outcomes. They discovered that this technology was more favourably seen in countries with lower power range and uncertainty avoidance than in countries high in uncertainty avoidance and power distance (Leidner et al., 1999).

Theme 4: Culture, IT Management, and Strategy

Eight studies examined the influence of national culture on IT management and addressed the question of how culture affects IT control and strategy. Kettinger et al.'s (1995) study concluded that service quality dimensions for the IS function differ between certain Asian and North American cultures. This is very significant as it proposes that Asian and North American IT organisations may have completely different attitudes regarding the means by which they provide high-quality services to their organisational stakeholders. Also, ninety-eight senior IT managers in Hong Kong were surveyed by Burn et al. (1993) and the results showed that cultural values may affect the types of IS issues observed to be the most critical by IT managers. Thus, IT issues considered most significant by US and other westernised managers may be entirely different from those of many other different cultures (Luftman and McLean 2004; Leidner et al., 1999). These findings provide reasonable evidence that cultural values may influence the types of IS issues perceived as most critical by IT managers.

Theme 5: The Impact of IT on Culture

This Theme focused on culture's impact on IT. Relatively few studies have examined the potential impact of IT on culture. For examples, Geographic Information System (GIS) implementation in India shows that GIS systems were initially rejected in India because the Indian culture did not value maps. However, over the course of time, there was an increasing awareness in India of the importance and usefulness of maps and map-based systems (Walsham, 2002; Leidner et al., 1999). Clearly, this example by Leidner (2006) and many other studies show reasonable evidence of IT impacting on cultural values.

Theme 6: IT Culture

This theme uses different conceptualisations of national and organisational culture values and the impacts of these values on IT-related outcomes. These values are developed over time through an individual's use of technology and lead to standardised ways of organisational data collection and processing, communication, and information and knowledge distribution. Understanding these IT values may contribute a much clearer picture for predicting how social groups perceive and ultimately respond to IT-based change. Others suggest that information technology is introduced with such values as rationality as well as order, system, and control (Leidner 2006).

The themes provided by Leidner (2006) show how different types of firm-wide and national values have an impact on information systems development, adoption, diffusion, use, outcomes, management and strategy.

2.2.4 Yi-Chi Lin's Work

Lin's thesis (2008) directly compares the Australian and Taiwanese cultures as they apply to the field of computer forensics. Yi-Chi Lin proved there were clear differences between the two different cultures based on his findings. He introduced the Hofstede phenomena: the first being that culture is not universal, and that cultural difference are nationally based, using 'national culture', to describe that each nation has its unique culture. The second phenomenon is that an individual's behaviour is indeed affected by his or her unique culture. Lin did not only discuss the Hofstede's concept of national culture but also used Hofstede's five dimensions of national culture to develop five dimensions for the study questionnaire and case studies. The five dimensions include: Current Situation Dimension, Policy and Organization Dimension, Education Dimension, Law Dimension, and Personal Preference and Skill Dimension. He used these dimensions as models to describe the latest computer forensic situations and to compare the differences between cultures in Australia and Taiwan (Lin's thesis, 2008).

Hofstede (2007) set the five dimensions for measuring national culture and used them to evaluate the scores for fifty-three different countries and three multi-country regions. Based on the explanations in Hofstede and Bond (1988), the scores are relative, and the distance between the lowest score and the highest score is about 100 points. According to Hofstede (1994), the scores of the first four dimensions for each country (or multi-country regions) were based on the findings of an IBM study, and the scores for the fifth dimension relied on the results of data collected from students within twenty-three different countries. Thorough explanations of the five dimensions (Power Distance, Individualism versus Collectivism, Masculinity versus Femininity, Uncertainty Avoidance, and Long-Term Orientation versus Short-Term Orientation) can be found in Hofstede, 1994.

Lin's study concludes that in both countries where Australian common law and Taiwanese laws are designed, there are two very different perspectives on various societal foundations. The differences are so extreme that these cannot be easily mapped, as there are many stages and processes in each that the other lacks. The cultural principles behind the responses from the two countries are based on different societal precepts. Australia and Taiwan have different structures in place for policing; this is born out of different overall policing structures and organisations. Neither Australia nor Taiwan outsources their forensic analysis, but the reasons behind this are different, and there is a cultural aspect. Whereas Australia has multiple policing agencies and jurisdictions, each dealing with electronic evidence, Taiwan has a central computer forensic laboratory that analyses all computer forensic evidence within the country. While Australia seeks to foster relationships with local universities and academia, Taiwan has a greater respect for experts that originate from other nations (Lin, 2008).

Again, this work has shown that, while there is many a similarity between the state of policy and organisation between Australia and Taiwan, these are the result of different cultural underpinnings and perspectives. There are also some very large differences between the two countries, and much of this organisational variation comes from a combination of geographical and cultural differences.

Moreover, Yi-Chi Lin shows that Taiwan and Australia consider the trustworthiness and reliability of digital data differently from each other. Australians place a higher value on digital data than Taiwanese computer forensic experts, and this has potential consequences in cross-jurisdictional operations. Australian culture emphasises the value of scientific implementation, and this is reflected in research, specifically when the outcome is implementation-based, while Taiwanese culture tends to focus on short-term objectives. These different attitudes are certainly due to cultural influences.

This research confirms two points: the first being that culture is not universal, and the second being that it corroborates the relationship between culture and computer science applications, asserting that culture has an impact on the application of computer science.

2.2.5 A Maghaireh's work

Digital evidence cannot be easily understood by humans and thus requires an interpretation by equipment, and/or software is necessary for the understanding of digital evidence. The definition also confirms this point of view of digital evidence as provided by the National Institute of Justice. For this reason, this definition furnished by the National Institute of Justice would be used as an 'official' definition of digital evidence (Ball, C, 2008).

Maghaireh (2009) argues that the general principles of search and seizure in criminal investigations have failed to be applied efficiently when investigating cybercrime. This is because the existing laws in developing countries such as in Jordan do not fit smoothly within cyberspace and the scope of computer systems is beyond traditional approaches to criminal investigation. The classical laws are accordingly neither able to adequately protect and fulfil the interests of both law enforcement agencies and the cyber-suspects, nor third parties' privacy rights. Australia and the United States were selected for comparative study as they are already well advanced in their experiences of and in their

legal responses to cybercrimes. His study shows the numerous differences related to cultural between these three countries, which will be discussed in details in this chapter.

Jordan's legal response towards pornography started from a different premise compared to Western countries. While the latter shows a serious concern for the production, display or possession only of child pornography, because of its harmful ramifications for both children and adults who watch such materials (Grabosky and Smith,1998), the Jordanian legal system, backed by cultural and religious doctrines, generally prohibits all forms of pornography (Maghaireh, 2009). Child pornography has received much attention recently from different sociologists, criminologists, media practitioners and legislatures, as reflected by the enactment of child pornography prevention laws. However, it appears that there is no definitive parameter of who a child is among countries because of differences in their cultural, social and religious values. For example, in the USA, the age of consent for girls is 18 years, while it is sixteen in Australia and fifteen in Jordan. As a result of significant differences in definitions and criminalization, what constitutes child pornography varies considerably between countries (Moyes, 2003; Majid Yar, 2006; Maghaireh, 2009).

Western nations experience significant challenges, in balancing between protecting individual privacy, allowing freedom of expression, and protecting children from sex offenders. While Jordan is completely different from Australia and the USA regarding banning offensive internet content, Jordan does not face any serious challenge from any party to its prohibition of all forms of the dissemination of pornography. This is due to the Jordanian legal system's being backed by cultural and religious principles, which generally prohibits all forms of pornography (Maghaireh, 2009). Moreover, neither physical nor cyber-stalking behaviour has been observed in Jordan. This is because tribal and religious traditions rule the sexual act within the Jordanian community (Maghaireh, 2009).

Furthermore, Maghaireh (2009) surveys and analyses laws passed to address different digital evidence admissibility in a courtroom between Jordan, Australia and USA. Also, he examines the judiciary's role in admitting the digital evidence. He shows that

Jordanian laws express the inadequacies which need to be addressed if legislation is to achieve its objective of admitting the digital evidence. The inadequacies are both legislative and non-legislative, in both technology and litigation support, and also education and training. From a legal point of view, digital evidence admissibility is scattered over a broad range of statutes which lack uniformity and comprehensiveness. Jordanian laws (the Electronic Transactions Law and Evidence Law) require completeness as they demonstrate an incomplete understanding of digital evidence. The Electronic Transactions Law only admits electronic contracts and messages that are generated, sent, received or stored electronically. Meanwhile, the Evidence Law only reveals e-mails and other computer stored evidence. As a result, many types of computer generated evidence, such as log files, metadata, and hash value is beyond the ambit of the Electronic Transactions Law 2001 or the Evidence Law because they are neither electronic contracts, nor messages in the meaning of the Electronic Transactions Law (Maghaireh, 2009).

Ian Maghaireh (2009) concludes that the Jordan court system and the judges' knowledge of technological issues (including digital evidence features) is immature, and far from meeting the USA or the Australian level. This is because of the rarity of studies addressing cybercrime issues and lack of opportunity to adjudicate. The Australian and the USA legislatures amended the rules of evidence to include digital evidence. The amendment was necessary to bring the classical rules of evidence, such as the Best Evidence Rule, into line with information technology developments.

2.2.62 Summary of section

These four studies show wide differences of religion and culture in different societies (US, China, Jordan and Australia). These various religion and cultures have different impacts on the way they regard different science and attitudes toward its application in the daily lives. Literature, not only illustrates the relationship between culture, and different sciences, but also demonstrations that there could be a significant and interesting issue between culture, religion and digital sciences, which is worthwhile to study. Furthermore, it shows that the legal enforcement professional's perception of evidence could be affected by some religion beliefs on modern evidence.

2.3 Saudi Arabian Culture, Religion and Law

In this section will focus on the similarities and the differences between the cultures and religions studied in the literature and the SA culture that will be studying in this thesis. To identify the specific factors of culture and religion in SA that will explain how and why scientific results in general and digital forensics in particular will impact the legal process and the legal practice in Saudi Arabia.

2.3.1 Saudi Arabian Culture

Before 1963, the system of government and administration in Saudi Arabia was extremely simple (Al-Mutairy, 2002). The King was the dominant figure and directly ruled the kingdom with his advisers. In 1953, the latter was formalised into a Council of Ministers, which has gained further authority in subsequent years. In the early 1960s, the country turned to outside advice for assistance with establishing a more modern administration (Al-Mutairy, 2002). As a result, some ministries and a civil service system were established. A board was set for the Civil Service, and an institute of public administration was also created.

The law in the Kingdom of Saudi Arabia is derived from the Qoran, and it is thus different from countries that do not declare Islamic law. In line with this, for men to associate and adhere to the principles of Islam, it is essential for them to have read and understand the Holy Qoran and the Sunna (sayings and doings) of the Prophet Muhammad. Furthermore, Saudi Arabian culture has been influenced by the role of history, and its traditions which makes it different from other cultures (Alkahtani, H, 2013). Culture in Saudi Arabia has an impact on daily lifestyles, ways of thinking, education, management decisions and management behaviour (Harissi Y, 2013). There are numerous Saudi Arabian cultural differences such as language, hierarchy, gender communication, fear of losing face, and favouritism, which may impact on Information communication systems

(ICT) and can have strong impacts on the success and security of the society (Alkahtani, H, 2013).

The Arabic language could cause communication problems as it is not related to any other language and is very different from Chinese, Hindu, Russian, European languages and most importantly English which is used by most technology. The language boundary between two cultures such as Arabic and English can arise when the language is not translated properly, as this can give misinformation (Nikzad, N, 2013). Also, the Arabic language is "bi-directional" as it uses right-to-left (RTL) script with Left-to-Right (LTR) elements, such as numbers. This is very important particularly in the process of translating a product, content or application from one language to Arabic because it needs careful thought and resource planning when undertaken (Nikzad, N, 2013).

Also, the interpretation of the Islamic culture in Saudi Arabia is physical as it is necessary to separate gender in society and workplaces. Man and women who are not related should not have direct contact with each other. Frequently, women in Saudi Arabia are allowed to work in male/female organisations only if there is no direct contact with men (Ali, A. J., and Schaupp, 1992). For institutions, such separation does have an impact on the performance of duty provisioning, if only through the duplication of services for differing genders. Following the Saudi culture, direct communication between males and females is not allowed and the result is poor communication between female employees and male employees who control most of the everyday work in Saudi Arabia (Alkahtani, H, 2013).

Saudi Arabian culture is firmly hierarchical in nature; for example, students and workers do not mostly use their ideas to take action. Seniors, teachers, and managers are the ones who give the ideas and direct their followers to take action (Alkahtani, H, 2013). Therefore, the organizational and institutional structure in Saudi Arabia focuses on strong hierarchical structures. In these structures, the seniors' job is to make decisions which should be implemented down the chain of command by subordinates. That is a very clear difference between Saudi Arabian and Western cultures, as whatever is considered a

micromanagement in Western culture could be perfectly normal in Saudi Arabian culture (Alkahtani, H, 2013). A supervisor who makes no specific job requests to be performed by subordinates would face immediate problems (Ali, A. J. and Schaupp, 1992). Quite frequently, Saudi leaders spend the majority of their time away and request their assistants to do their jobs either by phone conversation or through email. It is of great importance for subordinates to show respect to managers and not to question their authority (Ali, A. J., and Schaupp, 1992). Usually, seniors who have greater decisions making power must provide whole and specific directives to others to complete necessary tasks. It is challenging for most institutes because it limits productive thinking and causes the employees to wait to be informed on what to do, rather than proactively making decisions on their own (Ali, A. J., and Schaupp, 1992).

In a discussion of Saudi culture, nepotism must be mentioned. Nepotism is favouritism of a relative or a friend by those with power in organizations or institutes. In general, Arabs highly value and respect friendship and family relationships. In organisational settings, favours are based on mutual benefit and trust is a way of improving these cultural conditions. Family and individual relationships take precedence over other governing factors. According to Atiyyah (1993), family and individual connections are more influential than other governing factors in the Saudi Arabian organisational environment. Few Saudi employers like to hire those whom they do not know and trust; consequently, it is supported and trusted for managers to hire and promote family members or friends (Fischer and Manstead, 2000) and managerial decisions are often affected by the desires of the family (Atiyyah, 1993). This type of practice has both negative and positive aspects (Atiyyah,1991). Some believe it could help in developing powerful connections with employees. Nevertheless, this could lead to issues relating to ‘unproductive employees’ (Ali, A. J., and Schaupp, 1992), and it could reduce the performance of the institutions. In such an environment, the employees could reflect that taking a higher position is not certainly a result of acting harder but by having a good relationship with organisational leaders. That can lead to resentment amongst other employees and reduce the efficiency of the organisations performance (Atiyyah, 1991). Nepotism could also drive

managers to hire inexperienced employees in sensitive positions, such as in digital forensics and information security departments, which then puts the security of information at risk (Alkahtani, 2013).

The concept of 'losing face' in Saudi Arabian culture is about more than being embarrassed. Losing face means not maintaining the dignity and the respect of others. In Saudi Arabian culture, people spend their entire lives trying to build their political prestige and respect, while also trying to avoid causing anyone else to lose theirs. They gain 'face' through individual achievement, but also more by promoting social harmony and by being seen as helpful (Alkahtani, 2013). In Saudi Arabian culture, avoiding confrontation and conflict is preferable and dignity and respect are qualities that are key factors affecting behaviour. Honour and respect are pronounced in Saudi Arabia through face- saving acts such as compromise, patience and self-control (Sabbagh, 1996). Arabian culture utilises the concept of face to solve conflicts and to avoid embarrassing or discomforting others. These cultural factors mean that any security problems tend to be ignored and 'brushed under the carpet' as to admit to any susceptibility would amount to accepting a criticism and losing face (Alkahtani, 2013).

Saudi Arabia is a newly developed nation with an economy which has developed quickly with its oil resources. This expansion has been noted in the rapid expansion in ICT as well. According to the annual report of the Communication and Information Technology Commission in Saudi Arabia, eight hundred million US dollars was spent by the government in the first phase of the implementation of the Country's e-Government program (ENLASO, 2011). Accordingly, the number of internet users in Saudi Arabia has increased from one million in 2001 to 18 million in 2013. The government is investing in developing a high quality of government services in order to promote an attractive environment for foreign investments (ENLASO, 2011).

However, this rapid expansion has shown that there are very limited ICT systems and security experts in Saudi Arabia. People are frequently unconscious of IT security problems and how to find solutions to these problems. This is made worse because Saudi

people in general are very trusting and are unable to accept that an unknown person would want to do any harm to them and their systems (Alkahtani, 2013). Furthermore, most people favour accepting management jobs so as to improve their status. Clearly, jobs involving manual labour would not be accepted by most Saudis and they consider these to be uncomfortable positions (Curry and Kadash, 2002). Unfortunately, this attitude prevails despite whether they are qualified and suitable for such position - which has been caused by most of the positions being given through nepotism. Many people in senior management positions in Saudi Arabia are unprepared and unqualified for their positions. Due to the fear of losing face, these people are afraid to discuss this obstacle. Obviously, this has led to negative effects on ICT management and IT security (Alkahtani, 2013).

The literature shows wide differences between Saudi Arabian culture and the Western world. These different cultures have different impacts on the way they regard science and its application in the daily lives of the members of any particular culture. The questions which now arise are whether legal enforcement professionals' perception of evidence have also been affected by cultural beliefs, whether the KSA Criminal Procedure Law (CPL) is sufficient to govern the process of gathering digital evidence in scientific procedures, and whether it can stand alone in such a culture or if it needs additional guidelines.

2.3.2 Saudi Arabian Religion and Law

2.3.2.1 Overview

Saudi Arabia is a religious country - Islam provides a framework for the laws and government for its people. Islamic law is the basis of the Saudi legal system, and the government derives power from the Holy Quran and the Prophet's traditional sayings (Basic Law of the Government, 1992). Shariah, literally meaning "the way", is the term given to identify Islamic law, mainly based on the verses of the Holy Quran and the teachings and practices of the Prophet Mohammed (the Sunna). God said in the Holy Quran: "We made for you a way, so follow it, and not the fancies of those who have no knowledge". The Saudi legal system draws on both general and specific sources. Its general sources are religious, while specific sources deal with the modern theory of administration (Ansary, A. 2015).

The general sources are in order of priority (Ansary, A. 2015):

The Quran: This is the very word of God Almighty - a complete record of the exact words revealed by God through the Angel Gabriel to the Prophet Muhammad. The Quran deals with all the important aspects of human life, including the relationship between God and people and between people and society, including ethics, jurisprudence, social relations, justice, politics, law, morality, trade and commerce.

The Sunnah: This is the second source of the Saudi legal system. It is a complementary source to the Quran. It helps to explain and interpret the Quran, but it may not be interpreted or applied in any way which is inconsistent with the Quran. The Sunnah includes everything, other than the Quran, which has been transmitted from the Prophet Mohammed (PBUH): what he said, did, and agreed to. When the Quran is silent regarding any matter or topic, Ulema (Scholars) resort to the Sunnah.

Ijma: This refers to the consensus of opinions, or Al-Ijma, is the third source of law. It is a way of discovering the law by resorting to the general consensus of opinion among Ulema or Shariah Scholars of a particular era. The prophet stated that if all Muslims agree on a matter, then it cannot be wrong.

Qiyas: When the Ulema (scholars) fail to find a resolution from the Quran, Sunnah, or Ijma, they may use Qiyas or analogical reasoning from principles established in the Quran or Sunnah. For example, modern "recreational" drugs are not explicitly mentioned in the Quran or Sunnah. However, alcohol is mentioned and is prohibited because of its effects on the body and mind, in that it impedes a person's ability to perform his/ her religious obligations. The same "harm" is at issue in the case of drug-taking as of drinking; thus, the same rule (prohibition) is applied.

In Saudi Arabia, any law or regulation must not conflict with the above sources. Besides the above general legal sources, there are many legal instruments that directly rule the administrative life of the country. Some of them are reserved for the King because of his legal status and some are issued by the King in his capacity as head of the Council of Ministers. The King, as a president, has almost all the power he needs to direct the country. His power is legitimate so long as he acts according to the Shariah. He is also chief of the executive and the legislative authorities of the government, acting as his own Prime Minister. He is also the Commander-in-Chief of the Armed Forces. The King, therefore, has power over all administrative, legislative, and executive authority in the Kingdom (Basic Law of the Government, 1992). The modern sources of the legal system are Royal Decrees, Royal Orders, Council of Ministers' orders, and ministerial regulations and circulars.

2.3.3 Saudi Arabian Court System

The Ministry of Justice, established in 1970, is responsible for administering the country's judicial system and the Minister of Justice is appointed by the King from among

the country's most senior Ulama (Group of men with religious education and in religiously related professions who convey the true content of Islam to both the people and the rulers). He is the de facto Chief Justice. Legal material takes many forms but can be classified under three main sources: Islamic Law, Statutory Law, and Royal Orders. The application of Islamic law in Saudi Arabian courts is based mainly on the rules of the Islamic Shariah as interpreted by the Hanbali School, the fourth orthodox school of law within Sunni Islam (Ansary, A. 2015;). The existence of one school of Islamic law in the Kingdom, however, did not remove differences in rulings and procedures, leading to further difficulties in obtaining an authoritative legal opinion (Saudi Ministry of Foreign Affairs, 2015; Ansary, A. 2015). The diversity of interpretations continued due to variations in opinions and philosophies amongst the scholars of the Hanabli School of Islamic law. To date, no formal code, legislation or enactment has been promulgated by the Council of Ministers, the Shura Council or the King to codify criminal law, family law, legacy or inheritance and many aspects of the Islamic law of contracts. It is worth mentioning that there is a controversy over the "codification of Islamic law", which has been strongly opposed by traditionalists who support the application of Islamic Law, as laid down in the Quran and the Sunnah and understood by the Prophet's noble companions, with the help of explanations provided in traditional jurisprudential sources (Ansary, A. 2015; Otto, Jan Michiel, 2010).The Law of the Judiciary organizes the court system in the following hierarchical order (Ansary, A. 2015:

High Court:

The High Court found the previous Supreme Judicial Council's central role as the greatest authority in the judicial system. The High Court exercises its power via specific circuits (criminal, personal status, commercial and labour, as required) comprising three-judge panels, except for the criminal division, composed of a five-judge panel, which reviews judgments in particular types of cases involving Qisas , Hudud and Tazir punishments (Ansary, A. 2015; Otto, Jan Michiel, 2010).

Courts of Appeal:

The Law of the Courts of 2007 included courts of appeal as a safeguard, enabling them to overturn judgments by inferior courts. The Law empowers one or more courts of appeal in each of the Kingdom's regions. Each court functions through specialised circuits containing three-judge boards, except for the criminal section which reviews judgments in cases involving certain major offences, providing those taking Qisas , Hudud and Tazir punishments. Courts of appeal consist of labour, commercial, criminal, personal status and civil circuits (Ansary, A. 2015).

First-Degree Courts:

First-degree courts consist of general, criminal, commercial, labour and personal status courts and include specialised circuits containing enforcement, approval and traffic circuits. They are made of individual- or three-judge judges as defined by the Supreme Judicial Council (Ansary, A. 2015; Otto, Jan Michiel, 2010). Also, the Supreme Judicial Council determines the jurisdiction of the single-judge general courts (Ansary, A. 2015; Otto, Jan Michiel, 2010). Nevertheless, without prejudice to the Law of the Board of Grievances of 2007, courts usually have authority to give decisions regarding all disputes and offences by the jurisdictional court rules as outlined in the Law of Procedure before Shari'ah Courts and the Law of Criminal Procedure of 2013. The first-degree consist of:

General Courts:

General courts have jurisdiction in all claims and cases not under the jurisdiction of other courts, notaries public or the Board of Grievances. According to article 31 of the Law of Procedure before Shariah Courts of 2013, general courts have jurisdiction over the following (Ansary, A. 2015):

Lawsuits involving property, disputed ownership thereof, a right relative thereto or faults on the part of the owners or beneficiaries thereof and lawsuits to restrain interference with possession or for recovery of possession, vacation, payment of rent or contribution thereto, unless otherwise stipulated herein;

a) Issuance of title deeds or registration of endowments;

b) Lawsuits arising from traffic accidents or violations of the Traffic Law or its implementing regulations

c) Criminal Courts

d) The criminal courts consist of the following specialized circuits: Qisas (retaliatory punishment), Hudud (Quranic prescribed punishment), Tazir (discretionary punishment) and juvenile circuits (will be disabused in more ditties in next chapter).

Personal Status Courts

The personal status, labour and commercial courts comprise specialized circuits as needed and consist of one or more judges as specified by the Supreme Judicial Council

Labour Courts

According to article 34 of the Law of Procedure before Shariah Courts of 2013, labour courts have jurisdiction over the disputes relating to employment contracts, wages, labour rights, occupational injuries and award of compensation in respect thereof

Commercial Courts

Commercial courts have jurisdiction over all commercial disputes, whether principal or consequential, arising among traders.

Enforcement Courts

The Enforcement Law contains provisions that affect all aspects of the enforcement of domestic and foreign judgments as well as arbitral awards. It also defines the jurisdiction and powers of the "enforcement judges", who will play a key role in the enforcement of civil judgments and awards in the Kingdom.

2.3.4 The judiciary in Saudi Arabia

In Saudi Arabia, the essential Law of Governance demands courts to "…apply the laws of the Islamic Shariah in the cases that are brought before them, in accordance with what is ordered in the Qur'an, the Sunnah and statutes decreed by the Ruler which do not contradict the Book or the Sunnah." (Ansary, A. 2015; Otto, Jan Michiel, 2010). The purpose of Islamic law in the Saudi Arabian courts is based mainly on the rules of the Islamic Shariah as interpreted by the Hanbali School, the fourth Islamic school of law within Sunni (Ansary, A. 2015; Otto, Jan Michiel, 2010). Though Saudi judges usually adhere to the Hanbali Academy of law, they apparently use a particular degree of consideration in adjudicating cases and are forced solely by their consciences in determining the will of God (Trumbull C, 2006). A Saudi judge is "guided ... not only by the rules of fiqh (Islamic jurisprudence) faith but also, by his judgment of the texts of the Qur'an and Sunnah that support those rules; he believes that his judgment comes directly from those texts, not from the Hanbali books" (Vogel. 2000). The judicial judgments of Saudi judges are legally valid and cannot be controlled unless they oppose an evident rule of the Quran or Sunnah or dismiss statements or sources applied by higher courts. Saudi judges apply "ijtihad" to give judgments in cases not included in the terms of the Shariah. In such cases, they use Islamic jurisprudential means (e.g. analogy) applied to the sacred sources. In addition to the rules of the Islamic Shariah, a vast range of statutory laws have been applied in criminal, administrative and commercial fields as required by the Kingdom's development (Ansary, A. 2015; Otto, Jan Michiel, 2010).

In Saudi Arabia, the judiciary has the power to identify and accept evidence according to the case before them. In criminal procedures, evidence helps to recognise the wrong that has been presented. This provides connections to the accused and material of the criminal act. Furthermore, it shows the connection between the defendant and the evidence. The court's responsibility is to perform and understand legislation. Judges can reach a decision through the examination of any evidence (Al-Tahawi, 2002). Any method can approve the crime under the Saudi Arabia criminal system as long as it does not conflict with Islamic law - this is the general rule of the system. This evidential freedom

allows judges to choose what is regarded to be a more trustworthy manner to reveal the truth. The doctrine is that judges may not determine a case based on personal belief, opinion or emotions. The rules of law have to be followed by judges in reaching decisions and those decisions are to be based on logical justifications. The Court of Cassation may not challenge the way in which the judges take decisions, as it is not in their capacity to review the decision. Nevertheless, the court may consider whether the judge has followed the precedents and made a logical judgment. Although a judge is not required to provide a justification for his understanding, he is responsible for supporting his decisions with inferences. A judge is required to provide information about the previous decision that he used as a precedent to reach his judgment. There is no need for a judge to provide the details of why he has used that evidence. For the decision, a judge is not bound to establish facts, but it is his responsibility to provide evidence to support his conclusion. At all grades, in dealing with criminal matters, the judiciary is bound by the doctrine of freedom of proof and judicial understanding in reaching their decisions (Ahmad Al-dajani, 2010).

As the Islamic Shariah is the main authority for Saudi courts, a judge is required to have a high level of education, knowledge and understanding of socio-cultural issues and must be equipped with the tools of Ijtihad, as well as specific professional skills that will lead to reasonable, fair and impartial judgments. The Law of the Judiciary requires each judicial candidate to hold a degree from one of the Shariah colleges in the Kingdom of Saudi Arabia. According to the Saudi Ulama, the purpose of such education in Saudi universities is to produce ulama capable of varying degrees of ijtihad (Vogel. 2000). A candidate may hold an equivalent certificate, although he is required to pass a special examination set by the Supreme Judicial Council (The Law of the Judiciary 2007). To enable judges to attain the highest levels of education, the Kingdom has established a Judicial Academy and an Institute of Public Administration to train judges, enhance their expertise, develop their skills and provide them with the information that they need to function effectively. In addition, to ensure a smooth transition from the current to the new judicial system, the Law of the Judiciary requires all criminal, labour and commercial first-degree and appellate court judges in all the Kingdom's provinces, governorates and

districts to undergo at least two months training in commercial, labour and criminal procedural laws and other relevant regulations (Ansary, A. 2015).

In summary, in Hudud offences (prescribed punishments), the judge cannot change these punishments, reduce them, or increase them. Whenever a person is found guilty of a crime that has a prescribed punishment in Islamic Law, the prescribed punishment must be carried out to the letter (Ansary, A. 2015). This kind of punishment can only be carried out by a confession or the testimony of reliable witnesses. These punishments cannot use modern technological means of producing evidence against the criminal such as DNA analysis or other forms of evidence (Shabana A, 2014). Scholars said the legal principle is: "Prescribed punishments must be rejected when there are doubts surrounding the case". With modern technological methods such as DNA testing and digital evidence, there is always a chance for mistakes in the analysis or the collection of the sample while Islamic law seeks to conceal people's mistakes. Therefore, judges rely on reliable witnesses more than on modern technology where there is a chance for error (Shabana A, 2014).

It is worth noting that in the case of Hudud offences, even when a man apparently admits to committing a crime then retracts his/ her confession, his retraction will be accepted. He/she will not be guided to the designated punishment for the crime he had admitted to doing. Since the prescribed punishment cannot be applied to him, his punishment must either be adjusted to a lesser one at the judge's choice, or he may be discharged without punishment (Bassiouni C. 1982). This guides judges to be flexible in the meting out of punishments if Islamic law does not explicitly state penalties for the crime. Apart from Hudud offences, it is left for the judge to decide on the punishment at his judgment by taking into consideration many factors. The judge in such cases is then free to use modern methods for producing evidence against the alleged offender. However, depending on the strength of the modern methods used to prove the evidence, the judge may apply a lesser discretionary punishment. The Islamic Law Complex of the Islamic World Organization has decreed that: "…there is no legal objection to using modern technology in criminal investigations and in considering it as evidence in the crimes that

do not obligate the court to carry out a prescribed punishment. This can be gleaned from the Sunna. Avoid prescribed penalties when there are doubts" (Al-Shuaybi N, 2012).

2.3.5 Anti E-Crime Law in Saudi Arabia

Section Nine of the Law of Procedure before Shariah Courts provides the judge with the power to identify which evidence is to be considered material to the case. Also, article 124 allows the court, when required, to appoint one or more experts. It will define the job of the expert, the time for placing his report and the time for the trial hearing based on the record. However, article 134 clearly states that the experts' opinion is not binding on the court, which merely uses it as a guide.

With the rapid growth of the IT in Saudi Arabia, the need for anti-Cybercrime law was raised a few years ago. In 2007, the Anti-Cybercrime Law was issued under the Council of Ministers Decision and approved by Royal Decree. The KSA Anti-Cyber Crime Law punishes any illegal use of digital devices (see Appendix). While the existing Telecom Law and its Bylaws provide a real basis for the control of telecommunication service providers in the Kingdom, neither it nor its Bylaws address e-crime entirely. E-crime has not been clearly defined in any of the existing legislation. While the Anti E-Crime Act prohibits a certain type of content in electronic messages, it does not explicitly address the issue of unsolicited commercial messages, considered to be a primary form of e-crime. Although licensing agreements exist with ISPs, Bluetooth message providers and Bulk SMS Service Providers, significant gaps exist in the ability of the existing terms and conditions to address digital evidence effectively. With the above analysis, we understand that there are no specific guidelines for digital evidence and digital forensic investigations in KSA at the time of writing.

The anti-commercial fraud law and the Anti E-Crime Act establish a suitable basis for prosecution of digital evidence involved in publishing illegal content, including misleading and fraudulent advertisements, pornographic and sexual content as well as content that breach the privacy of other individuals in the Kingdom. While SAMA provides Internet Banking Security guidelines, there are no explicit instructions published

as yet on the manner in which phishing related issues need to be addressed by the Banks, both concerning user education and awareness, as well as reporting phishing cases. Indeed, a formal procedure for reporting phishing complaints is being developed currently in conjunction with the Banks who provide user education and awareness guidelines. It is considered that weaknesses in the Anti E-Crime Act enforcement mechanism, resulting from the lack of formal coordination mechanisms between MOI and CITC and the absence of IT Crime investigation specialists, could limit the effectiveness of addressing phishing crimes.

According to Elguindy (2012), "The "hacked" Saudi "Anti-Cybercrime law" or their "special cybercrime system" cannot be considered complete cybercrime law. It lacks privacy articles, freedom of speech, and there are no particular methods to examine such crimes. The law does not cover any definition of cybercrime and cyber-related offences, and there is also disagreement among various articles. According to this law, several online actions could be interpreted as cybercrime due to unclear definitions. From the above analysis, it is clear that there are no specific guidelines for digital evidence and digital forensic investigations.

Having reviewed laws considered relevant in the context of addressing e-crime and its effects in Saudi Arabia, we have highlighted the fact that there is no Privacy Law in Saudi Arabia to control the misuse of e-mails and mobile numbers, obtained for specific purposes by organisations in the Kingdom, for the purpose of SPAMming (CITC, 2007).

While the existing Telecom Law and its Bylaws provide a real basis for the control of telecommunication service providers in Saudi Arabia, neither it nor its Bylaws address spam entirely. While there are existing licensing agreements with ISPs and Bulk SMS Service Providers, there are significant gaps in the terms and conditions in the context of its ability to address e-crime fully (CITC, 2007):

a) The Electronic Transaction Law was not considered directly relevant to the e-crime issue

b) While the Anti E-Crimes Act does deal with certain aspects of e-crime, particularly the sending of offensive messages from a content perspective, spreading viruses, and phishing, it falls short of addressing the SPAM issue adequately in that it:

   i. Does not clearly determine and deal with SPAM

   ii. Does not explicitly deal with particular forms of SPAM, such as fax SPAM

   iii. Does not explicitly indicate if explicit, implicit, or inferred consent of the receiver is a requirement for sending commercial advertisement messages

   iv. Does not stipulate if unsolicited commercial messages can be considered SPAM

   v. Does not state the minimum requirements for legitimate business messages (such as the unsubscribe option for users) to request the sender not to send such SPAM anymore.

2.3.6 Summary of the section

The literature shows that Saudi Arabia is a religious country - Islam provides a framework for the laws and government for its people. The law in the Kingdom of Saudi Arabia is derived from the Qoran, and it is thus different from countries that do not declare Islamic law. In line with this, for men to associate and adhere to the principles of Islam, it is essential for them to have read and understand the Holy Qoran and the Sunna (sayings and doings) of the Prophet Muhammad. Furthermore, Saudi Arabian culture has been influenced by the role of history, and its traditions which makes it different from other cultures (Alkahtani, H, 2013). Also, there are wide differences between Saudi Arabian culture and the Western world such as language, hierarchy, gender communication, fear of losing face, and favouritism, which may impact on Information communication systems (ICT). These different cultures have different impacts on the way they regard science and its application in the daily lives of the members of any particular culture. The questions which now arise are whether legal enforcement professionals' perception of evidence have

also been affected by cultural beliefs, whether the KSA Criminal Procedure Law (CPL) is sufficient to govern the process of gathering digital evidence in scientific procedures, and whether it can stand alone in such a culture or if it needs additional guidelines

2.4 Chapter Two Summary

The four related works discussed in this chapter confirm that culture and religion are the two main factors which affect cognitive development. Culture is universal in the sense that every society has its culture, but culture is not always the same across all societies. The argument presented here is that different cultures have different impacts on the way its members regard science and its application in their daily lives. Religion and culture can affect an individual's mindset, way of thinking and attitude toward all that is new to society.

Slay's (2000; 2008) works focus on the issues of culture and science in education. She extends her review to issues such as culture, military systems and security. Maghaireh's (2014) work examines Jordan's needs for law reform in comparison with Australia and the United States, given that they are already well advanced in their experiences of (and in their legal responses to) cybercrimes. Leidner (2006) reviewed 51 articles which examine cross-cultural studies of Information Technology and established six themes, adoption, diffusion, use, outcomes, management and strategy. These common themes show how different types of firm-wide and cultural values have an impact on information systems development, , Lin's (2008) studies directly compare the application of Australian and Taiwanese cultures on computer forensics. concluding that in both countries where Australian common law and Taiwanese laws are designed, there are two very different perspectives on various societal foundations. The differences are so extreme that these cannot be easily mapped, as there are many stages and processes in each that the other lacks.

These works are powerful illustrations of the relationship between culture and different sciences. However, these studies do not cover all perspectives of the relationship between culture and science, since an investigation into culture-related issues could be an extensive study by itself. These works are, however, helpful in clarifying some of the underpinning concepts of this study.

The rapid increase in wealth and economic development with oil discovery in Saudi Arabia has led to changes in lifestyle and culture. This expansion has been noted in the rapid expansion in ICT as well. This rapid expansion has shown that there are very limited ICT systems and security experts in Saudi Arabia (Alkahtani, H, 2013). There are numerous Saudi Arabian cultural differences such as language, hierarchy, gender communication, fear of losing face, and favouritism, which may impact on Information communication systems (ICT) and can have strong impacts on the success and security of the society (Alkahtani, H, 2013).

Islamic law is the basis of the Saudi legal system, and the government derives power from the Holy Quran and the Prophet's traditional sayings. In Saudi Arabia, any law or regulation must not conflict with the above sources. Also, there are many legal instruments that directly rule the administrative life of the country. Some of them are reserved for the King because of his legal status and some are issued by the King in his capacity as head of the Council of Ministers. The King, as a president, has almost all the power he needs to direct the country. The purpose of Islamic law in the Saudi Arabian courts is based mainly on the rules of the Islamic Shariah as interpreted by the Hanbali School, the fourth Islamic school of law within Sunni (Ansary, A. 2015; Otto, Jan Michiel, 2010). In Saudi Arabia, the judiciary has the power to identify and accept evidence according to the case before them. Judges can reach a decision through the examination of any evidence and the methods can be approved as long as they do not conflict with Islamic law. Therefore, the judge is required to provide information about previous decisions used as a precedent to reach judgment. In regard of the Anti-Cybercrime Law, it was issued as late as 2007. The KSA Anti-Cyber Crime Law punishes any illegal use of digital devices, while the existing Telecom Law and its Bylaws provide a real basis for the control of

telecommunication service providers in the Kingdom, but neither it nor its Bylaws address e-crime entirely.

In summary, the four related works discussed in section 2.2 and Saudi Arabian culture and religion discussed in section 2.3 show that culture and religion are important factors that affect the relationship between the legal system of a country and science, more specifically, digital science. They also show that culture is universal in the sense that every society has its culture, but culture is not always the same across all societies. Moreover, these works support the argument that different cultures have different impacts on the way they regard science and its application in the daily lives of the members of any particular culture. Religion and culture can affect an individual's mind-set, way of thinking and altitude toward all that is new to society. The legal enforcement professionals' attitudes could be largely affected by government legislation, regulation and overlapping responsibilities. Consequently, these findings are important for this study to answer the research questions; in what way and to what extent do Islamic religion and Saudi culture affect the status of digital evidence in the legal process? What principles do the practitioners have to observe in the way they treat digital evidence in the judicial proceedings? How do digital forensic practitioners resolve this apparent conflict in practice?

Chapter Three

DIGITAL FORENSICS IN LEGAL PRACTICE

3.1 Introduction to chapter three

The objective of this chapter is to examine the role, status validity, integrity and the admissibility of digital evidence in western law. It demonstrates the particular characteristic features and inherent risks associated with digital evidence from both technical and legal perspectives. The nature and characteristics of digital evidence will be examined for their effects on evidence admissibility. The chapter then evaluates the relationship between procedures and guidelines in the UK (ACPO), USA (NIJ) and the procedures and guidelines that are needed for Saudi Arabia, (since they do not yet exist), which would take into account the specifics of Islamic law. This chapter is divided into two sections; the first examines the cybercrime investigation approaches in developed countries, and the second section is an analysis of digital forensic guidelines and principles in developed countries. This chapter serve to identify what the practitioners have to observe the way they treat digital evidence in the legal process, and how culture and religion factors could influence the status of digital evidence. Lastly, to what extent are judges likely to recognize different kinds of digital evidence in developed countries?

3.2 Cybercrime Investigation Approaches in Western Countries

Cybercrime in a broader sense (computer-related crimes) covers any illegal behaviour dedicated by, or in relation to, a digital system or network; such as illegal ownership and offering or distributing information by means of a computer system or network (Williams K, 2004). Cybercrime and digital security are hardly to be separated in a consistent environment. The United Nations General Assembly's (2010) declaration on digital security addresses cybercrime as one major challenge (Gercke M, 2012). However, the term "cybercrime" is used to refer to a huge number of criminal behaviours; it is not easy to develop a classification for such crime (Gordon, 2003). One way of possibly classifying cybercrime can be found in the Convention on Cybercrime, such as the fourteen acts proposed by Bureau of the Expert Group on Cybercrime (BEGC, 2013) used by the UN. Though there are many crimes such as child pornography can be prosecuted in most if not all jurisdictions. While, there are many other cybercrime acts which are forbidden in Islamic societies not listed by BEGC – e.g. any sort of female body exposure is consider pornography. Furthermore, slander, gambling, adult pornography, sale of alcohol, and abuse of religionist-scholars are prohibited in Islam. However, these could be acceptable behaviour in some other societies as part of personal freedom. This example not only illustrates the relationship between religion, culture and cybercrime, but also shows that this is a significant and interesting issue worth studying.

Digital devices hold huge amounts of evidence that is worth investigating, but can be quite hard to handle. The volumes of data stored in the devices increases with time as some of them can store terabytes of data (BEGC, 2013). However, very few items in this huge mixture might be really relevant to a crime case. These features create difficulties in extracting, correlating and translating practical and significant portions of data and information that may be necessary for improving the understanding, interpretation and resolution of a case. Consequently, digital evidence (DE) requires uniform and proven methods for searching, handling, validating and analysing data (BEGC, 2013).

3.2.1 Cybercrime

Prosecuting cybercrime offences can be technically complicated and legally complex. Fast advancements in the development of ICT and the natural differences between legal systems worldwide are severe challenges to the responders, investigating authorities, forensic interrogators, prosecuting agencies, and administrators of criminal justice (BEGC, 2013).

With increases in the reports of serious cybercrime, we can expect to see an equal increase in conviction rates (Kaspersky Lab, 2015). Though this is a widely accepted view, this has not been the case - with many investigations and prosecutions failing to get off the ground (Zavrsnik, 2010). The primary reason for this outcome is due to trans-jurisdictional barriers, subterfuge, and the failure of stakeholders in legal enforcement systems to follow significant aspects of technology supporting an offence. Similarly, given that science influences the efficiency of forensic inquiry, the capacity of investigators, prosecutors, judges and jurors to understand the illegal use of technology also instantly impacts conviction rates (Leibolt, 2010). However, technical specialists, police, criminologists, national security experts and lawyers recognise the concept of 'cybercrime' differently (Brown C, 2015). It is frequently unclear whether the term cybercrime refers to technological, legal or sociological aspects of crime, and a universal definition remains slippery (Brown C, 2015).

According to the ACPO, 'cybercrime' involves the, "…use of a network, Internet technology or computer to commit or facilitate the commission of crime" (ACPO, 2011). The Bureau of the Expert Group on Cybercrime (BEGC, 2013) proposes 14 acts that may constitute cybercrime, classified into three broad groups. The list of acts below was also used in the questionnaire sent to states, private sector entities, and intergovernmental and academic organisations for information gathering for the study of the problem of cybercrime.

Table. 1 Fourteen acts that may constitute cybercrime, proposed by the Bureau of the Expert Group on Cybercrime (BEGC, 2013)

Acts against the confidentiality, integrity and availability of computer data or systems
• Illegal access to a computer system
• Illegal access, interception or acquisition of computer data
• Illegal interference with a computer system or computer data
• Production, distribution or possession of computer misuse tools
• Breach of privacy or data protection measures
Computer-related acts for personal or financial gain or harm
• Computer-related fraud or forgery
• Computer-related identity offences
• Computer-related copyright or trademark offences
• Sending or controlling sending of Spam
• Computer-related acts causing personal harm
• Computer-related solicitation or 'grooming' of children
Computer content-related acts
• Computer-related acts involving hate speech
• Computer-related production, distribution or possession of child pornography
• Computer-related acts in support of terrorism offences

According to the United Nations' study on Cybercrime (BEGC, 2013), the eighty-two countries which were examined confirm widespread criminalization of the 14 cybercrime acts included in the questionnaire, with the main exception of spam offences and, to some extent, offences concerning computer misuse tools, racism and xenophobia, and online solicitation or 'grooming' of children. Also, the study reported that more than 80 percent of European countries have sufficient criminalization of cybercrime acts, while 60 percent of countries in the other regions of the world have insufficient criminalization of cybercrime acts. In the developed world, such as the UK, Australia and the USA for instance, the numbers of trials involving digital evidence have increased enormously because of the rapid escalation of cybercrimes. 571 UK and US lawmakers responded positively by addressing technological developments that affect the existing laws, and adopted provisions that recognise digital evidence.

The above fourteen acts were proposed by the Bureau of the Expert Group on Cybercrime (BEGC) and used by the UN. The offences of child pornography, terrorism and hate speech were given specific attention by the UN. Apart from these, there are many other acts which are forbidden in Islamic societies not listed (for example, female body exposure is considered pornography). Furthermore, slander, gambling, adult pornography, sale of alcohol, and abuse of religionist-scholars are prohibited in Islam. However, these could be acceptable behaviours in some societies as part of personal freedom. This example not only illustrates the relationship between culture and cybercrime, but also shows that this is a significant and interesting issue which is worth studying.

3.2.2 The Nature of Digital Evidence

Since the initial principle of digital forensics is to supply lawful, valuable, and convincing digital evidence for a courtroom, the role of digital evidence is clearly important in the field of digital forensics. According to Wang (2007), the difference between digital evidence and physical evidence is that each examining action would be treated as 'Access' in the collection of digital evidence, as it is easy to change the content

of digital evidence and so disqualify the criminal facts. Consequently, it is understood that the nature of digital evidence is unstable. In addition, this also shows that the features of digital evidence are very different from the characteristics of physical evidence (Barbara, 2005).

Barbara (2005) said the main difference between digital evidence and physical evidence is "…there is no actual 'physical evidence' in the traditional sense to collect visually. The evidence is digital, consisting of '0's' and '1's', which cannot be seen by the naked eye for relevance or collection purposes". This statement explains that digital evidence cannot be read and understood easily by humans, meaning that interpretation software and/or equipment is required for analysing digital evidence. Testimony may be necessary to describe the examination process and any process limitations.

There are a number of accepted definitions which have been specified by leading authors and organizations in the field digital forensics as to what 'digital forensics' actually means. Such as "Any data stored or transmitted using a computer that supports or refutes a theory of how an offense occurred or that addresses critical elements of the offense such as intent or alibi." (Casey, 2011)

The usage of the terms, "computer based electronic evidence" and, "digital evidence" by ACPO is equalizing. By defining computer evidence in relation to the investigative process, rather than in relation to the legal process, the ACPO definition addresses digital data from the time it becomes a part of an investigation (Sommer P, 2012).

3.2.2.1 Reliability of Digital Evidence

In the past, the majority of legislation in the US and the UK followed the first approach, instructing courts to evaluate computer-generated records by the reliability of the system and process that generated the records (Casey, 2011). For instance, the section in the Federal Rules of Evidence (901.b.9) titled, "Requirement of Authentication or Identification", includes, "Evidence describing a process or system used to produce a result

and showing that the process or system produces an accurate result" (Casey, 2011). In the United Kingdom, under Section 69 of the Police and Criminal Evidence Act 1984 (PACE), there was a formal requirement for a positive assertion that the computer systems involved were working properly (Casey, 2011). The rationale for this method is that records of such a type are not the equivalent of a statement by a human declaration that should ideally be tested by cross-examination of that declaration. Moreover, they should not be accepted as hearsay evidence, but rather their admissibility should be determined by the reliability and accuracy of the process involved (Strong, 1992).

According to Casey (2011) when dealing with the contents of writing, recording, or photography, courts sometimes require the primary evidence. The original purpose of this rule was to ensure that decisions made in court were based on the best available information. With the availability of effective identical duplicates through the use of computers, scanners, photocopiers and other technology, copies became acceptable in place of the original. However, these would not be accepted if, "a genuine question is raised as to the authenticity of the original or the accuracy of the copy or under the circumstances, it would be unfair to accept the copy instead of the original" (Casey, 2011). Digital evidence might not be accepted if it contains hearsay because the speaker or author of proof is not present in court to verify its truthfulness (Casey, 2011).

Hoey (1996) stated that the evidence is hearsay where a statement in court repeats a statement made out of court to prove the truth of the content of the out of court statement. Similarly, the evidence contained in a document is hearsay if the material is produced to show that statements made in court are true. The evidence could be excluded due to the significant features of the evidence; the accuracy of the out of court declaration (oral or documentary) which cannot be tested by cross-examination. For instance, an e-mail message may be used to prove that an individual made certain statements, but cannot be used to demonstrate the truth of the statements it contains (Casey, 2011). Though there are several exceptions to the hearsay rule to accommodate evidence that portrays events quite accurately, it is easier to verify than other forms of hearsay. For instance, the U.S. Federal

Rules of Evidence specify that records of regularly conducted activity are not excluded by the hearsay rule (Casey, 2011).

According to Casey (2011) the Irish Criminal Evidence Act, (1992), similarly, has gives an exception in Section 5(1): "… information contained in a document shall be admissible in any criminal proceedings as evidence of any fact therein of which direct oral evidence would be admissible if the information:

a) Was compiled in the ordinary course of a business,

b) Was supplied by a person (whether or not he so compiled it and is identifiable) who had, or may reasonably be supposed to have had, personal knowledge of the matters dealt with,

c) In the case of information in non-legible form that has been reproduced in permanent legible form, as reproduced in the course of the normal operation of the reproduction system concerned".

Although some courts evaluate all computer-generated data as business records under the hearsay rule, this approach may be inappropriate when a person was not involved (Casey, 2011).

Table: 2 Scale for Categorizing Levels of Certainty in Digital Evidence as following (Casey, 2011)

Certainty Level	Description/Indicators	Commensurate Qualification
C0	Evidence contradicts known facts	Erroneous/incorrect
C1	Evidence is highly questionable	Highly uncertain
C2	Only one source of evidence is not protected against tampering	Somewhat uncertain
C3	The source(s) of evidence are more difficult to tamper with but there is not enough evidence to support a firm conclusion or there are unexplained inconsistencies in the available evidence	Possible
C4	(a) Evidence is protected against tampering or (b) evidence is not protected against tampering but multiple, independent sources of evidence agree	Probable
C5	Agreement of evidence from multiple, independent sources that are protected against tampering. However, small uncertainties exist (e.g., temporal error and data loss)	Almost certain
C6	The evidence is tamperproof or has a high statistical confidence	Certain

According to Casey (2011), the main advantage of this Scale it is flexible enough to measure the evidential weight of both the process that generated a piece of digital evidence

and its contents. Another advantage it is easily understood by non-technical people as it is non-technical.

Governments worldwide have shown marked reluctance to scrutinize the effectiveness of state-controlled mechanisms for investigating and prosecuting serious instances of cybercrime offending. More than a decade ago, Susan Brenner contended that the, "justice system's inability to prosecute cybercrime cases is a sign that it is not functioning effectively in this area" (Brenner, 2004; Brown C, 2015). The related in-depth research reveals that Brenner's assertion is as relevant today as it was back then. A combination of factors has converged to impede criminal justice processes in common law countries worldwide. Also, Brown (2015) highlights the primary challenges presented by cybercrime for the administration of criminal justice as detailed in the following section:

Identification

1. Difficulty in attributing ownership and authorship to electronically stored information.
2. Difficulty in identifying individuals in control of information systems and devices.
3. Inability to expediently locate relevant information amongst large sets of data.
4. Ineffectiveness in tracing criminal activity when data anonymization and obfuscation techniques have been employed.
5. Widespread availability of data sanitization and device wiping software for consumer devices which may lead to destruction of evidence.

Access

1. Inability to obtain authorization for conducting online inspection and collection of remotely stored data, particularly if the target host is a cloud service provider with a base of operations outside the jurisdiction of local authorities.
2. Delays in processing requests for Mutual Legal Assistance due to bureaucratic stumbling blocks.

3. Inability to acquire data due to advancements in consumer security on commodity devices, including strong encryption, open source privacy tools, and anti-forensics technologies.
4. Legislation which compels manufacturers and service providers to give investigating authorities access to electronically stored information is becoming redundant. Companies are relinquishing the means to unlock devices and decode data. It is technically infeasible for courts to compel foreign manufactures to create keys to comply with local laws.
5. Penalties imposed by courts in circumstances where defendants refuse to comply with orders to disclose decrypted data are ineffective. Where serious criminal offending is involved, an offender is unlikely to turn over the key to incriminating data, particularly if they are likely to be punished.

Wellbeing

High performance pressure and stressful working conditions for criminal justice officers may lead to staff burnout.

1. Prolonged exposure to obscene material may create mental health issues for investigators, prosecutors, and forensic interrogators.
2. Staff welfare may be overlooked and investigations derailed in policing environments when non-technical managers are appointed to supervisory positions without substantive experience, overseeing cyber crime inquiries or attending to the rigours of digital forensic casework.

Liability

Interference with commercial operations when warrant activity is executed in business environments may lead to substantial claims for damages.

1. Unintended damage to information systems and devices (when investigators seize exhibits or perform analysis on commercial equipment) may expose law enforcement agencies to civil litigation.
2. Disclosure of private, confidential, or legally privileged information during an investigation may lead to criminal, civil and/or internal administrative legal proceedings for criminal justice officers and departments involved.

Policies and processes:

1. The willingness of law enforcement agencies to commit resources to the prosecution cybercrime offending may depend on the extent to which an investigation or prosecution is congruent with existing policy preferences, public priorities, or political agendas.
2. Documented operating procedures are necessary to guide the handling of electronic evidence by investigating authorities. When this documentation is not available for inspection during legal proceedings, serious questions may be raised about the consistency and transparency of internal police processes.

Retrieval and Retention

Ephemeral or volatile sources of electronic information which are not collected from live systems during warrant activity may substantially weaken a case in the eyes of the court, or lead to miscarriages of justice.

1. Service providers who do not respond to authorized requests for production and preservation of data may cause the loss of critical evidence

Admissibility and Fairness

Chain-of-custody documentation which is incomplete or inaccurate may result in electronic evidence being classified as inadmissible.

1. Law enforcement agencies which are unable to attest to the reliability or authenticity of electronic information may thwart the efforts of legal counsel to introduce that material as evidence in court.

2. Investigating authorities and expert witnesses who exhibit insufficient objectivity may weaken the credibility of evidence that is presented in court.

3. Analysts and investigators who are unable to dedicate time towards identifying exculpatory sources of evidence may undermine the strength of a case or cause miscarriages of justice.

4. Defendants that are unable to afford forensic support to test investigative findings and challenge expert opinions may be wrongly convicted.

Human capital

Law enforcement officers and prosecutors without the technical expertise needed to manage cybercrime cases, may contribute towards the acquittal of cybercrime offenders who pose a substantial threat to public safety.

1. Analysts who are not qualified to operate technical equipment or extract data from information systems may contaminate evidence and severely undermine the credibility of forensic reports led in support of police investigations.

2. Agencies without sufficient in-house subject matter expertise will undermine the ability of prosecutors to introduce expert evidence that explains the technical underpinnings and relevance of material before the court.

Technical Resources and Funding

Police who are not equipped with specialized tools for extracting information, or furnished with sufficient computational power to expediently process data, may miss critical evidence during analysis in the laboratory or while performing triage in the field.

1. Courtrooms that are not fitted with the modern technology required to effectively present electronic evidence during legal proceedings may degrade the clarity and persuasiveness of the testimony.

Training

Police officers, prosecutors, and members of the judiciary that are not provided with the following will be manifestly ill-equipped to manage cybercrime cases: on-going training which is focused on modes of criminal offending, diplomatic channels of cooperation, foreign mechanisms of justice, sovereignty issues, emerging sources of electronic information, and general communication technologies.

Underreporting and Uncertainty

Public misconceptions about the capacity of police to target cybercrime offending contribute to the problem of underreporting.

1. Gaps in legislation and administrative delays owing to judicial uncertainty about the nature of cybercrime offending may prevent investigators from obtaining the requisite legal authority to intercept electronic data.

2. The defence counsel may seek to create confusion in the mind of an inexperienced judge or juror by raising nebulous legal and technical arguments to derail the prosecution's case.

3. Expert witnesses may mislead the trier of fact by overstating or understating findings.

Privacy and Privilege

Investigations may infringe upon fundamental human rights and lead to accountability failure if the judiciary is not sufficiently empowered to provide oversight.

1. The doctrine of legal professional privilege may delay investigations and add a layer of complexity to forensic interrogations and legal processes.

2. Emerging data protection and privacy laws worldwide are putting electronic information beyond the reach of investigating authorities.

Cooperation

Private sector entities that are slow in responding to requests for assistance or from police, or are generally dismissive of collaborative initiatives with law enforcement agencies, create barriers to cybercrime investigations, prosecutions, and digital forensics interrogations.

1. Strict and formal international mechanisms of cooperation may impede the agility of police investigations which target cybercrime offending originating outside national borders.

Legal Frameworks and Due Process:

1. Legislative provisions which are not harmonized among members of the international community may create safe jurisdictions for cybercrime offending, and possible conflicts of law.

2. Laws that are not drafted to encompass technology broadly within established categories of criminal conduct will rapidly become obsolete, thereby impeding the capacity of authorities to lead cybercrime investigations and run effective prosecutions.

3. Legislative time constraints pertaining to the examination of data on information systems may be insufficient given exponential increases in consumer storage capacity and the complexity of extracting records from devices. Consequently, large quantities of data seized by police may never be analyzed.

The above are the primary challenges presented by Brown C (2015) with regard to the inclusion of cybercrime in the administration of criminal justice and are very important factors for this study.

These factors will be used to respond to the following questions:

- In what way and to what extent do culture and religion affect the status of digital evidence in the legal process?
- What principles do the practitioners have to observe in the way they treat digital evidence in the legal process?

3.2.2.2 Complexities of Digital Evidence

This section discusses the challenges and the complexities that are faced if digital evidence is to be accepted in the courtroom. With digital evidence, like any form of indirect evidence, there are challenges to understanding more complex evidence artefacts recovered from a crime scene. Because of the technical complexity of digital evidence and its environment, some experience and specialized knowledge is required (BEGC, 2013). According to Saleem, (2015) these might includes the following:

Anonymity: Digital evidence can be more informative than physical evidence because it not only holds data but metadata. For instance, digital pictures of an incidence can contain information about when, how and where the incidence occurred. However, digital evidence mostly does not have any implicit information to tie it to its perpetrator. For example, a picture taken by a camera in exchangeable image format will contain actual bytes of data representing the image itself and metadata, such as location information, camera make and model, but no information about who took the image (Saleem, 2015). Nonetheless, there are a number of digital devices that are able to create very significant evidence such as digital signatures, video and audio (Harvey, 2011). Consequently, digital evidence is usually considered as circumstantial evidence in nature, as it is mostly difficult to refer a digital offence to an individual with only the information present in the digital devices (Casey, 2011).

Authenticity: Sommer (2012) defines the meaning of digital evidence authenticity as the recovered data which is the same as the original. Reed (1990) has defined the term more

precisely, noting that digital evidence is authentic only if it can satisfy the requirement of the courtroom with the following:

1. The content of the original is unchanged.
2. The data and information in it truly originates from the supposed source.
3. The associated metadata are correct and unaffected.
4. The essential level of authentication could be achieved by other circumstantial evidence or other technological features of the system or record.

With all these requirements, still there is no direct information to connect the digital evidence to an individual. Accordingly, it is obvious that the digital forensic process has many areas that could be improved, mainly the authentication of digital evidence (Yusoff, 2010). In the United Kingdom, examiners usually follow guidelines issued by the Association of Chief Police Officers (ACPO) for the authentication and for proving the integrity of evidence (ACPO, 2011).

Integrity: Mocas (2004) provided the definition of data integrity as, "Assuring that digital information is not modified (either intentionally or accidentally) without proper authorization". Moreover, Mocas (2004) redefined integrity as, "Assuring that, given a data set, the process of creating a duplicate of the data does not modify the data (either intentionally or accidentally) and the duplicate is an exact bit copy of the original data set". Duren and Hosmer (2002) provided a different perspective to achieve the integrity of digital evidence. They suggested using time stamps to ensure the integrity of digital evidence. Schatz et al (2006) state that, "Time stamps are increasingly used to relate events which happen in the digital realm to each other and to events which happen in the physical realm, helping to establish cause and effect". Ahmad (2002) stated, "the link between each log is crucial to the establishment of a complete chain of evidence. Across all of the links the crucial factor upon which the integrity of the entire chain rests is the authenticity of the time-line. If the accuracy of the time in any of the links is questionable then the entire chain is rendered useless". These statements confirm Saleem, (2015) argument that time stamping is the means whereby useful digital incidents may be linked to physical evidence in the real world.

Reproducibility: The importance of reproducibility is described in a statement made by Mocas (2004). He explained that, "…a key feature of science is that hypotheses are supported by reproducible experiments. Reproducibility strengthens the belief that a hypothesis is correct. Likewise, the reproducibility of investigative procedures lends credibility to the evidence produced". Then, Mocas (2004) define reproducibility as, "Assuring that, given a data set or set of devices, the processes used to gather and/or examine evidence from the data set or devices are reproducible."

Reproducibility is a concept which is not only important in the scientific field, but also significant in the field of digital forensics. Kenneally and Brown (2005) discussed the importance of reproducibility by stating that, "The volatile nature of computer networks and disk evidence and the potentially destructive nature of the analysis process make a convincing argument for investigators to not perform analysis on original evidence". This statement can be regarded as the major reason for digital forensic investigators to reproduce the original digital evidence, and to point out the demand of reproducing digital evidence (Saleem,, 2015). Therefore, digital forensic investigators have to take different approaches to find out the necessary information within an investigation, without the modification of the original digital evidence.

Wang (2007) further stated that, "…copying evidence stored inside the digital device requires a special tool and must be carried out bit by bit; this is to say, the data must be copied using a bit-stream-copy method, which provides copied information in exactly the same format as the original data. By using this bit-stream-copy method, the data obtained are given more probative force. The most important thing is that the evidence is not amended or changed during the copying process" (Saleem,, 2015). Based on these explanations, the complexities of digital evidence are revealed.

Abstraction of Reality: Computers have layers and layers of abstraction rather than the bare hardware with which they are really built (Ami-Narh, 2008). Farmer and W. Venema (2000) state that, "Abstraction makes computers easy to understand and thus easy to use. For example, a computer disk at physical level in a magnetic domain is actual but not very

accessible. There are then layers of abstraction over this physical layer, such as directories, contiguous files, disk blocks and so on, to the level of numbers and letters. These layers of abstraction are formed by software that may or may not have been tampered with" (Forrester, J, 2007). Using digital forensic tools to recover deleted files from a hard disk involves many layers of abstraction from magnetic fields to numbers and letters (Carrier, 2002). These layers of abstraction could lead to serious errors during the investigations which consequently impact on the reliability of digital evidence and thus its admissibility (Carrier, 2002; Forrester, J, 2007).

In conclusion, digital evidence is a huge, messy and slippery form of evidence, as it is quite hard to handle (Casey, 2011). The volumes of data stored in the devices increase with time as some of them are capable of storing terabytes of data. However, very few pieces of data from this huge mixture are really relevant to a case. These features create difficulties in extracting, correlating and translating practical and significant portions of data and the information which may be necessary for improving the understanding, interpretation and resolution of a case (Saleem,, 2015). Consequently, digital evidence requires uniform and verified methods for searching, handling, validating and analysing it. These methods must protect the integrity and authenticity of the digital evidence. Such well validated and well-tested methods surely will help to obtain related and weighty digital evidence and thus increase the chances of its admissibility (Casey, 2011).

3.2.3 Law Enforcement

Countries might prefer to limit the scope of their criminal jurisdiction to activities of perpetrators on their own national territory. They might focus on the prosecution of persons within their territory accessing content, irrespective of its source. They could as well attempt extraterritorial action against content producers. Such perspectives illustrate the growing extent of legal differences and approaches in the area of cybercrime (BEGC, 2013).

There is some difference between national laws which can be traced back to fundamental differences between culture, religions and legal schools. The main four legal schools include continental European law, common law, Islamic law, and mixed law (such as Chinese law) (BEGC, 2013).

Continental European criminal law is often characterized by abstract normative rules, systematic structures and a strong influence of academic thinking. Criminal law is usually extensively codified with penal codes also providing for general principles of criminal responsibility applicable to all forms of criminal behaviour (Weigend, 2011). Common law jurisdictions and substantive law provisions are more usually drafted in descriptive terms, ensuring both accessibility of law, and reflecting the strong position of lay judges within common law jurisdictions. Judge-made law was long the main source of the substantive criminal law and still remains an important element. Codification, however, is now a widespread norm, albeit sometimes through separate legislative acts rather than one single penal code (Volonino, 2004).

In common law, police play the principal role in the search for criminal action and have high independent powers (O'Connor, 2012). Usually, the search is started as soon as an offence is reported to the law enforcement system. Judges play an essential oversight in the procedure through the investigation steps, particularly when the police exercise conflicts with suspects' rights or other individuals' rights (Brown, 2015). The primary job of the police is to secure a warrant from a judge who then ensures that individual rights are given legal consideration as police seek to move ahead with an inquiry - this will be discussed more in the next section (Brown, 2015). The police are responsible for questioning victims, suspects, and witnesses. All the associated information is then usually gathered in a case file. In the case of minor offences, the police could charge the accused person and present the case later to the court. For cases involving serious crime, the police will cooperate with a prosecutor who assumes the main responsibility for determining the appropriate charges. In these cases, the police are accountable for securing and collecting evidence. In some countries applying the common law, the prosecutor could advise the police during the phase of evidence-gathering. It is the duty of the prosecutor to present the

charges to the court for confirmation and approval. Also, in the common law tradition, a defence lawyer plays an active role in guiding clients through police examination and performing on their behalf. Through the investigative phase, the lawyer could collect evidence independently and engage expert witnesses to help. Due to the adversarial nature of the common law system, the defence is provided full access to the case file and must be provided a reasonable chance to weigh all the evidence in advance of the trial. The process of 'discovery' or 'disclosure' is a formal legal function regulating the sharing of the legal evidence between the prosecution and the defence (O'Connor, 2012) The admissibility of evidence discussed here shows there are complex rules (Thaman, 2013). As the trial unfolds, the main protagonists are the prosecutor and defence lawyer. The judge's duty is to be as an impartial referee between the parties and is tasked with guiding the jury on concerns of law (Acharya, 2003). A common law trial could be a long process as witnesses are expected to present their evidence through 'live testimony' before the court (O'Connor, 2012).

3.2.4 Search and seizure

Incorrect methodology or unlawful search and seizure is performed during this initial process of the forensic investigation, that could affect the admissibility of the evidence negatively (Ami-Narh, 2008). The forensic investigator must, therefore, ensure that the privacy of a culprit is not violated in any search (BEGC, 2013).

In England and Wales common law, both before and after the passing of the Police and Criminal Evidence Act 1984, stated that, "...police cannot search a person's home to look generally for evidence against him. A legal entry into places for a search and seizure always should be linked to a clear, specified purpose and the search must be consistent with the stated purpose". Similarly, in the USA, the Fourth Amendment prohibits unreasonable searches and establishes a reasonable expectation of privacy in the conduct of all searches (Ami-Narh, 2008).

According to Casey (2011) the most common mistake that prevents digital evidence from being admitted by courts is that it is gathered without permission. A warrant

is required to search and seize evidence. As discussed above, in the USA the Fourth Amendment requires that a search warrant be secured before law enforcement officers can search a person's house, person, papers, and effects. Inspectors must demonstrate probable cause and detail the place to be searched and the persons or things to be seized to ensure a warrant. More specifically, investigators have to convince a judge or magistrate that in all probability:

1. A crime has been committed;
2. Evidence of the offence is in existence; and
3. The evidence is likely to exist at the place to be searched.

According to Casey (2011), search warrants in the United Kingdom and other European countries can be more loosely defined than in the United States. In the United Kingdom, for instance, there are several kinds of warrants (e.g., a specific premises warrant, all premises warrant, and multiple entry warrants), and they do not have to specify what things will be seized. The main exceptions that can allow a warrantless search in the United States are plain view, consent, and exigency (Casey 2011). If investigators see evidence in plain view, they can seize it provided they have obtained access to the area validly. By getting consent to search, investigators can perform a search without a warrant, but care must be employed when obtaining consent to reduce the chance of the search being successfully challenged in court. However, in most western democracies, national legislative provisions exist to enforce compliance with international human rights law, including the rights to privacy and freedom of opinion and expression (Brown C, 2015).

It is therefore understandable that search and seizure of digital evidence is a fundamental procedure which could be debated in the courtroom if the practitioners do not know the way they treat digital evidence in the legal process.

3.2.5 **Summary of Section**

Section 3.3.1 is focusing on cybercrimes with particular reference to the United Nations' study on Cybercrime (BEGC, 2013). The fourteen acts were proposed by BEGC show that the offences of child pornography, terrorism and hate speech were given specific attention by the UN. Apart from these, there are many other acts, which are forbidden in Islamic societies not listed (for example, female body exposure is considered pornography). Furthermore, slander, gambling, adult pornography, sale of alcohol, and abuse of religionist-scholars are prohibited in Islam. However, these could be acceptable behaviours in some societies as part of personal freedom. This example not only illustrates the relationship between religion and culture and cybercrime, but also shows that this is a significant and interesting issue which is supporting the argument; religion and culture have an impact on digital evidence and forensic.

The nature of digital evidence examined with particular reference reliability and complexities of digital evidence. The scale purposed by Casey (2011), for categorizing Levels of certainty in digital evidence discussed. The Nature of Digital Evidence was discussed in section 3.2.2, confirming that the nature of digital evidence is unstable and very different from the characteristics of physical evidence. In 2004 Susan Brenner stated that the, "…justice system's inability to prosecute cybercrime cases is a sign that it is not functioning effectively in this area". Similarly, Brown (2015) confirmed that governments worldwide have shown marked reluctance to scrutinize the effectiveness of state-controlled mechanisms for investigating and prosecuting serious instances of cybercrime offending. The evidence could be excluded due to the significant features of the evidence; the accuracy of the out of court declaration (oral or documentary) which cannot be tested by cross-examination. For instance, an e-mail message may be used to prove that an individual made certain statements, but cannot be used to demonstrate the truth of the statements it contains (Casey, 2011).

The law enforcement and the difference between national laws, and the fundamental differences between culture, religions and legal schools such as; European law, common law, Islamic law, and mixed law (such as Chinese law) (BEGC, 2013). This

section provided the background needed to understand the current situation in Western countries. These two sections served as guidelines in obtaining relevant historical data for the research and to answer the research question: In what way and to what extent do culture and religion affect the status of digital evidence in the legal process? What principles do the practitioners have to observe in the way they treat digital evidence in the judicial proceedings?

3.3 Digital Forensics Guidelines and Principles

This section evaluates the relationship between procedures and guidelines in the UK (ACPO), USA (NIJ) and the procedures and guidelines that are needed for Saudi Arabia, (since they do not yet exist), which would take into account the specifics of Islamic law. Also, discusses range of technical and scientific issues that might be considered universal and international within forensic digital investigations. These issues thus provide the foundation for a series of survey questions, for both survey and expert group case studies as we move on to explore the research question and consider the impact of culture and religion on digital forensics.

Saferstein (2009) defined forensics as a process of science to the discovery, examination, and affording of evidence to legal enforcements in criminal events. There are different fields of forensic science, such as medical, physics, chemistry and toxicology forensics, that provide scientific context by which to recognize the evidence. The assessment of scientific evidence not only needs an understanding of the scientific technique but also an understanding of the legal principles behind it. Digital evidence is unlike other forms of forensic evidence as it consists only of zeros and ones, while other evidence has an enormous signs (Kerr, 2005, 2005). This difference makes it very fragile and requires special treatment in terms of handling and explanation.

3.3.1United Kingdom Digital Forensic Group (ACPO)

The United Kingdom Digital Forensic Group (ACPO) is the oldest national group committed to computer evidence in the world (Radhakrishna G, 2008). The history of Chief Constables working jointly for the common good goes for many years. The County Chief Constables' Club was established in 1858, and in 1896 the Chief Constables' Association of England and Wales was created to serve the chief officers of urban forces. It was later on combined in 1948 to form the Association of Chief Police Officers (ACPO). In 1990, its constitution was formalised, granting that it should be funded by a levy on Home Office grants and police authorities. The ACPO became a company limited by guarantee, answerable to a Board of Directors in 1997. In 2013 the Home Office invested

more in the ACPO to bridge the gap between police authorities and the Police and Crime Commissioners (PCC).

The primary purpose of the ACPO is a professionally-led independent strategic institute that directs and coordinates the path and progress of the police service in the UK. Also, the ACPO works on behalf of all chief officers, organising strategic policing responses. The two primary functions of the ACPO are:

1. Operational coordination and national policing services: by providing governance, operational coordination, setting requirements, funding and support.

2. Performing as the professional voice of the service: the ACPO acts as the professional voice of the service, through representing senior police leadership at the national level with a broad range of stakeholders including government. It provides a professional forum for Chief Police Officers (not just Chief Constables) to share ideas, expertise, best practices and to coordinate resources.

3.3.1.1 Good Practice Guide for Digital Evidence

This Guide is accepted as the perfect best practice guide for digital investigations in the UK and many another places. The ACPO Computer Crime Working Group was the first to draught Good Practice "guidelines" for the search, seizure and examination of computer evidence. This guideline proved very successful, as it used a great approach to consolidate the different law enforcement, industries, and agencies' efforts and corral them in a particular effort: to collect intelligence, enforcement capability and build the right framework of policy and doctrine to allow entirely legal enforcements to tackle the major issues identified. The ACPO Working Group published a fifth version of the guidelines in 2011. This guide was improved from version 4, where it centred on computer-based evidence. This new revision reflects digital based evidence and tries to include the difference in the digital world. So, this guide does not only assist with law enforcement, but the wider family that assists in investigating cyber security incidents. This guideline is accepted in courts of England and Scotland, but they do not create a legal obligation, and their use is voluntary (Schultz, E. E., & Shpantzer G, 2010). The guidelines comprise of four fundamental principles that are explained in the original document:

Principle 1: "No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court".

Principle 2: "In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions".

Principle 3: "An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result".

Principle 4: "The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to".

The guideline stresses the need to preserve the four principles throughout the entire life cycle of digital forensics. The guidelines also include four sections/phases for digital evidence recovery, namely the plan, capture, analyse and present phases. In addition to this, it includes one section containing a general advice guide for the managers of e-crime investigations.

1. Capture section

This section is intended to assist individuals in ensuring their actions in relation to seizures are correct. In physical crime scenes, it is critical for the investigators to know that there are numerous types of digital devices that can be found in a crime scene which might hold data of value to the investigation. To preserve the data and achieve the best evidence, these items must be handled and seized appropriately, and should be treated with as much care as any other item that is to examined forensically. Also, this section explains the different steps and cautions needed to be taken before, during and after the seizure of digital devices. It emphasises the importance of recording all actions done with digital evidence to comply with Principle 3. The recording should include but not be limited to details of any

information provided by persons present, photographs/diagrams of equipment locations, and records of any actions taken at the scene.

2. Analyse section

The investigator should know that due to the quantity and complexity of data saved on digital devices, it is not feasible or desirable to extract all the data held on a device for review by investigators. Alternatively, a legal strategy needs to be formulated to enable the examination to be focused on the relevant data. The inspector is also required to consider the purpose and nature of the digital examination and know what priorities are placed on the examination, as it may well be that critical information needs to found to preserve evidence that may exist elsewhere. As with other forensic evidence, interpretation is often necessary to make sure the evidential weight of recovered digital evidence is clear. An investigator who undertakes the interpretation of digital data should be capable of doing so and have had adequate training to undertake the duty assigned to them.

3. Present section

The results of a digital forensic investigation could be presented through the following three ways:

1. Verbally to an investigator/officer throughout a case;
2. By a statement or report on conclusion of the case;
3. In court if witness evidence is needed.

The report involves presenting the digital evidence from a particular digital crime scene, and explanations, to the physical crime scene investigation team.

4. General considerations

In the general sections section, great attention was given to the following important issues:

1. Training and education
2. Welfare in the workplace
3. Digital forensic contractors

4. Disclosure

5. Related legislation

This guideline is a great effort from the UK government to address the requirements for a comprehensive, legally accepted, digital investigation process, and to facilitate the education, and application of the same. The guideline has provided the details of the investigative process in an inclusive, structured and reliable way. Abstraction is necessary for a generic framework, but by adding the appendixes at the end, they have also given the details, thus helping in the implementation of the guideline and improving upon the use of the tools and techniques. This instruction is useful and vital because:

1. It has the capability to be abstract and detailed at the same time,

2. It has the flexibility to minimise and expand as required,

3. Its matrix of tasks and objectives, which enables experts to focus on investigative goals rather than tasks, of which there are many. This matrix can become more complicated while capturing as much detail of the investigative process as possible. It can then help to provide automated decision support for selecting appropriate tasks for a specific investigative objective.

4. Identifying principles which should apply to the entire process rather than being cordoned off as distinct phases or steps and limiting their impact. These principles require overarching goals that may entail different actions during each phase of the overall investigative process.

5. Child pornography has received lots of attention, but not adult pornography and therefore a number of issues need to be considered when discussing guidelines in line with Islamic Law for digital forensics.

3.3.2 U.S. Department of Justice

Electronic Crime Scene Investigation: A Guide for First Responders, is the U.S. Department of Justice (2008), structured digital investigation framework. It is designed to respond to the digital crime investigation and is a reference for legal enforcement officers. The updated version (2008) consists of the following phases:

1. Preparation: Incident admitted as needing investigation, triggered by the detection of irregularities in a system, information about a crime and so on.

2. Collection: Obtain search warrant, prepare tools and techniques. Adopt strategy that maximises the collection of untainted evidence and minimises impact on victim.

3. Preservation: Includes taking action to stop or prevent anything that could harm how the digital information is handled. Consists of performances such as ending ongoing deletion processes, preventing people from using computers during collection, using the safest way to collect information.

4. Examination: Well-organized search of evidence about the incident being examined. Investigation of digital media, such as hard drives and floppy disks, CD-ROM's, backup tapes, and any other devices used to store data. Timestamps, log files, data files containing particular expressions may include as data objects.

5. Analysis: Evidence analysis is needed to distinguish the perpetrator of offence, defend copyrights and claim damages. Includes defining significance, replacing data fragments of data and forming some conclusions based on the evidence handled. May need the use of tools, and the test may need to be repeated to confirm the theory crime. Technical experience required to undertake an efficient analysis process.

6. Report: Translating, summarising and providing some conclusions on the analysis of the evidence. The presentation should be in a layperson's language.

This generalised process does not differentiate the computer from other digital devices, and there is little guidance concerning the actual examination and analysis of the

system (Carrier and Spafford, 2003). As it aims to concentrate on the first responders, it refers to the physical crime scene and to traditional forensics. Even though the method is rather systematic for the first three phases, it covers the examination, analysis and report in only one chapter. This alters it to a guideline for the crime scene and not a framework that could efficiently assist the computer forensics investigator. In addition, "…the US Department of Justice (DOJ) categorised digital evidence into two forms: Computer Crime and Intellectual Property Section Criminal Division, in 2002. Conversely, forensic experts classify digital evidence into three types" (Maghaireh A, 2009). According to the DOJ's manual, the first type is computer generated evidence, such as log files, cookies, metadata, IP addresses, and so on (Kenneally, 2005, Maghaireh A, 2009). This evidence comes in multiple formats, data and programmes, including e-mail, websites, chatting applications, etc. It needs particular multimedia devices in order to be presented to the court, such as devices used for streaming video and audio. The second type is computer stored evidence, such as digital photos and Word files. This form can be printed out as a hardcopy or visually displayed on a computer screen (Kenneally, 2005, Maghaireh A, 2009). Digital evidence could be accepted in court if certain criteria are met, such as; assuring the evidence has not been modified, and there is an auditable trail kept linking to the storage and examination of the original device. The main points of the handling and investigation of digital evidence are as following (Maghaireh A, 2009):

1. The actions that were taken to secure and collect the digital evidence should not affect the integrity of that evidence;

2. The expert conducting an examination of digital evidence should be qualified for that purpose;

3. Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review.

The ACPO and the U.S. Department of Justice were reviewed and discussed in distilled in this section. Based on the above review can be seen the importance of developing and implementing national digital forensics guidelines and principles to investigate cybercrime. These guidelines and principles secure the validity, the integrity,

and the admissibility of the evidence extracted from digital devices in cybercrime investigations.

3.3.3 Summary of chapter Three

Section 3.3.1 is focusing on cybercrimes with particular reference to the United Nations' study on Cybercrime (BEGC, 2013). The fourteen acts were proposed by BEGC shows that the offences of child pornography, terrorism and hate speech were given specific attention by the UN. Apart from these, there are many other acts which are forbidden in Islamic societies not listed (for example, female body exposure is considered pornography). Furthermore, slander, gambling, adult pornography, sale of alcohol, and abuse of religionist-scholars are prohibited in Islam. However, these could be acceptable behaviours in some societies as part of personal freedom. This example not only illustrates the relationship between religion and culture and cybercrime, but also shows that this is a significant and interesting issue which is supporting the argument; religion and culture have an impact on digital evidence and forensic.

The nature of digital evidence examined with particular reference reliability and complexities of digital evidence. The scale purposed by Casey (2011), for categorizing Levels of certainty in digital evidence discussed. The Nature of Digital Evidence was discussed in section 3.2.2, confirming that the nature of digital evidence is unstable and very different from the characteristics of physical evidence. In 2004 Susan Brenner stated that the, "…justice system's inability to prosecute cybercrime cases is a sign that it is not functioning effectively in this area". Similarly, Brown (2015) confirmed that governments worldwide have shown marked reluctance to scrutinize the effectiveness of state-controlled mechanisms for investigating and prosecuting serious instances of cyber crime offending. Hoey (1996) stated that the evidence is hearsay where a statement in court repeats a statement made out of court to prove the truth of the content of the out of court statement. Similarly, the evidence contained in a document is hearsay if the material is produced to show that statements made in court are true. The evidence could be excluded due to the significant features of the evidence; the accuracy of the out of court declaration (oral or

documentary) which cannot be tested by cross-examination. For instance, an e-mail message may be used to prove that an individual made certain statements, but cannot be used to demonstrate the truth of the statements it contains (Casey, 2011).

The law enforcement and the difference between national laws, and the fundamental differences between culture, religions and legal schools such as; European law, common law, Islamic law, and mixed law (such as Chinese law) (BEGC, 2013). These sections provided the background needed to understand the current situation in Western countries. These two sections served as guidelines in obtaining relevant historical data for the research and to answer the research question: In what way and to what extent do culture and religion affect the status of digital evidence in the legal process? What principles do the practitioners have to observe in the way they treat digital evidence in the judicial proceedings?

Section 3.3 shows some of the essential understanding of digital forensics, and discusses a range of technical and scientific issues that might be considered universal and international within forensic digital investigations. These issues thus provide the foundation for a series of survey questions, for both survey and expert group case studies as we move on to explore the research question and consider the impact of culture and religion on digital forensics. The United Kingdom Digital Forensic Group (ACPO) is the oldest national group committed to computer evidence in the world (Radhakrishna G, 2008). The history of Chief Constables working jointly for the common good goes for many years. The County Chief Constables' Club was established in 1858, and in 1896 the Chief Constables' Association of England and Wales was created to serve the chief officers of urban forces. It was later on combined in 1948 to form the Association of Chief Police Officers (ACPO). In 1990, its constitution was formalised, granting that it should be funded by a levy on Home Office grants and police authorities. The ACPO became a company limited by guarantee, answerable to a Board of Directors in 1997. In 2013 the Home Office invested more in the ACPO to bridge the gap between police authorities and the Police and Crime Commissioners (PCC).

The ACPO and the U.S. Department of Justice were reviewed and discussed in detail in this section. Based on the above review it can be shown clearly the importance of developing and implementing national digital forensics guidelines and principles to investigate cybercrime. Consequently, it shows the relationship between procedures and guidelines in the UK (ACPO) and the procedures and guidelines that are needed for KSA (since they don't yet exist), which would take into account the specifics of the Islamic laws.

Chapter Four

DIGITAL EVIDENCE IN ISLAMIC LAW

4.1 Introduction to Chapter four

The Islamic Worldview is atheistic and ethical worldview, which contrasts sharply with the secularist or atheistic alternatives. This worldview emanates from the fundamental belief that life and existence came into being as the result of the will, desire and design of the One and Only Creator (Hassan, 1994).

The Islamic world is not homogeneous regarding religious perspectives; rather it is heterogeneous, consisting typically of traditionalists, and reformists. The fundamental difference between Islamic schools is their understanding and interpretation of the Holy Scripture, and the Prophet's traditions (Parrillo, 2008). In most Muslim countries, Westernization began in the nineteenth century. This process had a significant influence in the different fields in general, and on law in particular.

This chapter aims to examine the Islamic law; in what way and to what extent does Islamic religion affect the status of digital evidence in the legal process? What principles do the practitioners have to observe in the way they treat digital evidence in the judicial proceedings? Also, this chapter will provide the base line to identify how digital forensic practitioners resolve this apparent conflict in practice.

Section 4.1 clarifies the meaning of Islam, Shariah, and Islamic (Shariah) Law, as they have a common root but have developed individually and are quite separate today. Also, the rules, principles, teachings and disciplines derived from the primary sources of Islam: the Quran and Sunnah are discussed and the legal structure governing Islamic law, communities and social norms are examined in this section.

Within Islamic law, there are different and specific set of offences, each type of these crimes are punished by specific penalties, as discussed in section 4.2. Section 4.3 examines the criminal procedure in Islamic law.

There are certain modes of proof in Islamic law and a special form of proof is needed

in order to be accepted in the court room, as reviewed in section 4.4.

4.2 Digital Forensics in Islamic Legal Practice

4.2.1 Islamic Law overview

It is worth starting by clarifying the meaning of Islam, Shariah, and Islamic (Shariah) Law, as they have a common root but have developed individually and are quite separate today. Islam means obedience to the will of God (Allah) and submission to His Law (Mukarram & Muzaffar, 2005). Shariah is the pathway to fulfilling the will of Allah. It is a comprehensive collection of rules, principles, teachings and disciplines derived from the primary sources of Islam: the Quran and Sunnah. On the other hand, Islamic law is the legal structure governing the interactions between communities, groups and social and economic organisations (Maghaireh, 2009). Islamic law shares the Anglo-American view that it is preferable to leave some guilty offenders to escape penalty rather than to allow an innocent person to be wrongfully convicted and punished (Bassiouni C. 1982; Maghaireh A, 2009).

Regarding legal practice in Islamic societies, Islamic scholars added two more sources to the Quran and Sunnah to form the primary sources of Islamic criminal law. The general sources are, in order of priority: Quran, Sunnah, the consensus of Islamic legal scholars (Ijma) and Analogy (Qiyas).

The Quran is the word of God: a complete record of the exact words revealed by God via the Angel Gabriel to the Prophet Muhammad. The Quran deals with all the important aspects of human life, the relationship between God and people and between people and society, including ethics, jurisprudence, social relations, justice, politics, law, morality, trade and commerce.

Sunnah: this is the second source of the Saudi legal system. It is a complementary source to the Quran. It helps to explain and interpret the Quran, but it may not be construed or implemented in any way which is contradictory with the Quran. The Sunnah includes everything, other than the Quran, which has been transmitted from the Prophet

Mohammed: what he said, did, and agreed to. When the Quran is silent regarding any matter or topic, Ulema (Scholars) resort to the Sunnah.

Ijma: It is an Arabic term referring to the consensus of opinions. Legally, it means the collective opinions of scholars in specific new legal or religion related issues, which are not stated in the Quran or Sunnah. Al-Ijma, is the third accepted source of discovering the answer for legal issues by resorting to the general consensus of opinion among Shariah Scholars (Kamali, Mohammad Hashim., 2003). The verse cited as a proof-text for 'joining together' is:

"But him who breaks with the Messenger after guidance has become clear to him, and follows other than the way of the believers, him We shall consign to what he had turned to, and roast in Jahannam - an evil home - coming." [Al-Qur'an 4:115]

Ijma might be implicit or explicit. Explicit agreement is when most of the scholars declare their opinion regarding a particular issue after it has been determined that they have been consulted to give dissension on the issue. Implicit agreement is when scholars divided to two groups - one offering their opinion on the issue, while others stayed silent about it. A large majority of opinions for which there is consensus are implicit ijma (Ali, Abdullah Hamid, 2014).

Qiyas: It means when the Ulema (scholars) fail to find a resolution from the Quran, Sunnah, or Ijma, they may use Qiyas or analogical reasoning from principles established in the Quran or Sunnah (Hashim K, 2003). When Prophet Mohammed sent one of his companions (Mu'adh ibn Jabal) to Yemen as a governor, he asked him: "How will you judge if you are asked to do so?" Mu'adh said: "I will judge according to the Quran." The Prophet ask: if you do not find it in the Quran?" Mu'adh answered: Then I will judge according to the Sunnah." The Prophet asked: "If you do not find it in the Sunnah or in Quran?" Mu'adh: Then I will exercise my opinion (Qiyas) and I will not be negligent with it." The Prophet then patted the chest of Mu'adh with his hands and said: "All praise is due to Allah who has guided the emissary of His Messenger towards that which He guided His Messenger" (Hashim K, 2003). The point here is that the Messenger clearly allowed

scholars to find a resolution for new issues by analogical reasoning from principles established in the Quran or Sunnah. For example, modern "recreational" drugs are not explicitly mentioned in the Quran or Sunnah, however, alcohol is mentioned and is prohibited because of its effects on the body and mind, in that it impedes a person's ability to perform his/ her religious obligations. The same "harm" is at issue in the case of drug-taking as of drinking; thus the same rule (prohibition) is applied. Also, the Council of Islamic Ideology declared that DNA profiling is adequate to be used as evidence in crimes but in specific conditions (will be discussed next).

The Islamic world is not homogeneous regarding religious perspectives; rather it is heterogeneous, consisting typically of traditionalists, and reformists. The fundamental difference between Islamic schools is their understanding and interpretation of the Holy Scripture, and the Prophet's traditions (Parrillo, 2008). In most Muslim countries, Westernization began in the nineteenth century. This process had a significant influence in the different fields in general, and on law in particular. In other Muslim countries, Westernization did not start until the second half of the twentieth century and the legal systems are much less affected by it - Saudi Arabia, Qatar and Yemen are the most prominent examples of such states. In these three countries, Islamic law was never ousted by Western law (Rudolph P, 2005).

According to Lippman (1989), Islamic criminal laws and the procedural safeguards not prescribed in Quran neither Sunna but left to the discretion of the ruler's, who is responsible for public welfare. Moreover, Awad (1982) added the ruler's formulation of procedural rulesis guided by various Quranic principles:

1. Respect for the individual is the central precept of Islam
2. Free men are equal before the law and are entitled to equal protection under the law
3. Judicial and governmental decisions must conform to the Shariah.
4. The law is not to be applied retroactively.

5. The accused is presumed innocent until proven guilty

6. Punishment fits the crime

According to Maghaireh (2009), although some Muslim clerics disparage secular legal systems that are applied in several Muslim countries, such as in Jordan and Egypt, they have not produced an alternative perspective other than vague and general ideas.

4.3 Islamic Criminal Law

In Shariah law, the objective of criminalisation and punishment is to protect five important values: religion, human life, intellect, lineage, and property. The criminalisation system in Shariah law is classified into three categories to protect these five essential values, Hudud, Qisa and Taazir. Islamic criminal law is distinct from those employed in most common law and civil law countries (Lippman M, 1989).

4.3.1 Hudud offences

Hudud offences are considered as crimes against God, whose punishment is specified in the Quran and the Sunnah (Practices of the Prophet Mohammed). As God's agent, the state initiates the prosecution of the accused. It usually refers to the class of punishments that are fixed for certain crimes that are considered to be "claims of God (Lippman M, 1989).:

a) Drinking alcohol
b) Theft
c) Highway robbery
d) Illegal sexual intercourse (generally defined by Islamic Law as unlawful sexual intercourse, i.e. intercourse between individuals who are not married to one another)
e) False accusation of iIllegal sexual intercourse
f) Rebellion against the ruler

4.3.2 Quias offences

Quias means to copy the other or to follow the path followed by the other. Legally, it means that if the Quran and Sunnah sources fail to provide a rule to address an issue, legal reasoning can be used to solve this problem, by establishing similarity (in the case and the intention of the law) to a matter on which a ruling does exist. For example, drugs

are not mentioned either in the Quran nor the Sunnah. However, religious scholars hold that the same legal basis exists as for alcohol, which is prohibited in both the Quran and Sunnah, that basis being the deactivation of the mind, and so drugs are also forbidden in Shariah. Regarding crime and punishment, the use of Quias is permissible. In general, its application as a source of Islamic legislation is considered sound in all injunctions that relate to criminal procedures or criminal policy (Lippman M, 1989).Furthermore, the law of Quias fulfils some of the objectives of the restorative justice movement by enabling victims to participate in sentencing and encouraging forgiveness and reconciliation.

4.3.3 Taazir offences

Taazir means chastisement and denotes offences for which the Quran or Sunnah does not prescribe a penalty. The judge's power to punish Taazir offences stems from the sovereign's duty to protect the public welfare. A Taazir offence threatens one of the five essential guarantees of Islam: the practice of religion, the development of the mind, the right to procreation, the right to personal security, and the right to possess property and wealth (Lippman M, 1989). There are four instances in which Taazir punishment is usually inflicted:

a) Taazir punishment is inflicted for acts which do not meet the technical requirements of Hudud or Quesas, such as theft of an item which is not of sufficient value to qualify as a Hudud offence, attempted adultery, or assault (Matthew Lippman M, 1989);
b) Criminal offences, generally punished by Hudud, which due to extenuating circumstances (such as theft among relatives) or doubt (a failure of proof at trial, such as insufficient witnesses), in practice often are punished by Taazir. In theory however, the judge is not authorised to exercise such discretion and must convict or acquit the offender (Lippman M, 1989).
c) Taazir punishment is applied for acts proscribed in the Quran and Sunnah or contrary to the public welfare which are not subject to Hudud or Quias, such as;

breach of trust by a public authority, false testimony, bribery, contempt of court, homosexuality, and misleading the public through sorcery, fortune telling, astrology, or palmistry (Lippman M, 1989).

d) The Taazir punishes several acts which violate social norms and mores, such as the use of obscenity, provocative dress, and loud and disorderly behaviour.

It is essential to mention here all kinds of crimes that are not addressed under Hudud offence and Quias offences can be punished under Taazir, including incomplete Hudud crimes (Rudolph, 2005). Furthermore, most of the new crimes including E-crime fall under Taazir offences. Nevertheless, cybercrime cannot be taken under this section unless the Shariah itself criminalises or otherwise prohibits such activities.

Shariah's approach to legislation is guided by an effective rule: 'No penalty is enforceable without textual evidence'. This rule shows that the legitimacy of crime and its punishment is based on textual evidence from both the Quran and Sunnah. The spirit of this rule is expressed in numerous Quranic texts. For example, God says: "And We never punish until We have sent a Messenger (to give warning)" (Quran, Al-Isra: verse 15). God also says, "And never will your Lord destroy the towns (populations) until he sends to their mother town a Messenger reciting to them Our Verses (Quran, Al-Qisas: verse 59).

Fundamentally, the guiding rules – 'No penalty is enforceable without textual evidence' – applies to crimes involving Hudud and Qisas penalties. Likewise, the applicability of the above rule is reflected even in Al-Tazir offences that attract the lightest to the hardest penalty – verbal advice to execution. Al-Ijtihad (the striving of a legitimate scholar to reach a religious verdict) related to such types of sentence requires some textual substantiation (Lippman M, 1989).. For example for Internet fraud, the textual substantiation needed for the application of Al-Tazir penalty is provided in the Quran and Sunnah prohibiting fraud and deception and criminalising the acquisition of wealth through unlawful means. God said in the Quran, "O believers! Do not consume one another's wealth through unlawful means; instead, do business with mutual consent" (Quran, Surah Alnisa: verse 29).

4.4 Criminal Procedure in Islamic Law

Not all Islamic states directly apply Shariah law. Many Arab nations have adopted legislative forms of criminal procedure, often derived from European codes, although influenced by Shariah law (Hashim K, 2003). Saudi Arabia is one of the rare Arab nations that directly applied Islamic law (Hashim K, 2003).

Shariah criminal procedure seeks to satisfy two primary goals; constitutional process and effective control of crime. Criminal procedure tries to accommodate protections for the accused while promoting society's interest in crime detection and prevention. The system focuses on efficient prosecution and conviction of the guilty while trying to minimise the possibility of unjust convictions. Shariah law has a role for individual rights, but those individual rights are exercised within a system that is primarily concerned with human relations (Abdal-Haqq I, 2006). To guarantee these take place, the system is engineered for simple, expeditious but just proceedings. The judge, rather than a prosecutor, investigates the case, even if police initiate the case (Siddiqui A, 1997).

Shariah law recognises the fundamental premise of innocent until proven guilty (Hashim K, 2003). Judges and law enforcement officials must be independent as the Quran demands it and the punishments must not be excessive in comparison to the crime (Adel Omar Sherif, 2003). Shariah law guarantees several other rights that are viewed as necessary for a just legal system, including the exclusion of illegally obtained evidence, right to confront the accuser, right to inspect evidence against the defendant, and right to cross-examine witnesses (Sherif A, 2003).

4.4.1 Right Against Self-Incrimination

A defendant cannot be forced to give a confession, and has the right to remain silent. A forced confession or confession taken under force is not admissible. A confession, once given, can be withdrawn even after the sentence has been given or during its execution. A valid confession cannot be given by a person who does not have full possession of his faculties. The judge must not blindly accept an offered confession, but must verify that the defendant's confession was not made merely to protect another person. For a confession to be accepted, the defendant must not only admit to the category of crime but must provide relevant details to support his assertion of guilt (Hussein G, 2003).

4.4.2 Right to Counsel

Shariah law recognises a defendant's right to be present at trial, or at a minimum, to be represented by an authorised person at trial. There is no explicit right to counsel under Shariah law. Before modern times, there was no perceived need for legal representation because legal scholars and experts were at the trial to actively assist the judge in deciding the case (Hussein G, 2003). Nothing in Shariah law precludes the defendant from using legal representation, and representation is routinely allowed. As the trial is not conducted in an adversarial fashion by a prosecutor, there is no imbalance if the defendant is not represented by a lawyer. The judge has a professional and religious duty to impartially investigate the case, so the defendant should be able to rely on the judge's impartiality (Hashim K, 2003).

4.4.3 Pre-Trial Detention

The system of pre-trial detention and release on monetary bail is generally not recognized under Shariah. Islamic jurists appear to agree that the accused should not be detained prior to trial since an accusation of guilt alone is not sufficient to justify an accuser's incarceration. Pre-trial detention also interferes with an individual's freedom of movement which is protected by the Quran (Hashim K, 2003).

4.4.4 Pre-Trial Interrogation

Under the common law, the accused has the right to refuse to answer questions and the accused's silence may not be used as evidence of guilt. The accused is to be treated humanely and is to be encouraged to deny his or her guilt. The Prophet coaxed a woman accused of theft to withdraw her confession: "Did you steal? I do not think you did. Say, no." Torture is prohibited in Islam: Prophet Mohammed warned his followers by saying, "God shall torture on the day of recompense those who inflict torture on people in life." Consequently, a scholar admonished that "It is better that they should face God with their offences than I should have to meet God for torturing them" (Lippman M, 1989).

4.4.5 Right to Present Evidence and to Assistance of Counsel

The Islamic criminal justice system recognizes the right of both the plaintiff and the accused to present evidence at trial and to have the privilege of being represented by counsel during pre-trial interrogation, at trial, and upon conviction, at the execution of the sentence. The privilege of counsel is based upon the Islamic theory of "protected interests" which guarantees an individual's freedom of religion; the right to self-preservation; freedom of thought, expression, and knowledge; the right to procreation; and the right to property. The accused has the right to attend all proceedings relating to the charges, to be informed of what occurs at proceedings which he or she fails to attend, and to be provided the opportunity to present rebuttal evidence to investigators (Bassiouni C. 1982).

4.5 Evidence in Islamic Law

4.5.1 Bayyinah (the clear evidence)

The Bayyinah (Evidence) in broad terms is anything that proves or disproves the offence presented in a courtroom. The primary purpose of illegal punishment in Islamic law is that an honest person should not be punished and a guilty person should not escape from punishment (Hallaq W, 2009). As everyone is presumed to be inherently innocent, only confident and convincing evidence can overcome this assumption. Islamic law has made it obligatory on the plaintiff to produce clear and reliable evidence in support of his case, and the courtroom is based on satisfying evidence. The standard rule of the burden of proof is that the weight of proof depends on the person claiming the affirmation of the issue and not upon the party who denies it. However, there are different kinds of evidence in Islamic law. In Hudud there are six fixed penalties and three accepted evidences such as the following (Hallaq W, 2009):

1. Death for murder, rape and for highway robbery;
2. Hand amputation for theft;
3. Death by stoning for illegal sexual intercourse (Zina) if the offender is married and 100 lashes for unmarried offenders;
4. Eighty lashes for an unproven accusation of being unchaste (Qadhf) and for the drinking alcohol.

The Quran states the main three types of evidence; oath, confession and testimony (Hasan I, 2011).

4.4.2 Confession (Iqrar)

An oath is a statement, (oral, written or using gestures) made by a person that he is under an obligation to another person in respect of some right of that person against him and which is raised by any person under any of the circumstances hereinafter mentioned (Hasan I, 2011). It is, therefore, a specific admission or acknowledgement as means of proof to indicate a right or interest of another against oneself, or to admit to an offence or

liability against oneself. It is relevant evidence in that it affects only the person making such a confession. Confession in Western common law is unlike Islamic law, as Islamic law divides Iqrar into two divisions; admission and confession with different scopes of idea (Webster 1983). A confession is a particular type of admission made by the accused stating or suggesting the inference that he committed the offence. An admission, on the other hand, is a statement that merely suggests any inference as to any fact in issue as a relevant fact, and which is made by any of the persons and under the circumstances (Hasan I, 2011).

4.4.3 Oath (Qasam)

According to Indonesian dictionary (Hallaq W, 2009) an oath is defined as:

1. A statement stated officially to witness to God or to something that is sacred (to strengthen the truth and sincerity, and so on).
2. The statement that accompanied the resolve to do something to corroborate the truth or dare suffer anything if the statement was not true.
3. The promise or pledge unwavering (will accomplish something).

Legally, if a plaintiff has no evidence then he will be called to take an oath, but if the defendant denies wrongdoing then the court will ask defendant to take oath and case will be decided in favour of defendant (Hallaq W, 2009).

4.4.4 Testimony (Shahadah)

Both Islamic and common law recognise that the testimony of witnesses plays an important role to ensure the facts before a court shall be proven. Testimony is second to confession as means of proof. That means, in the Islamic court when someone is accused of a particular crime and he denies it, then the burden of proof is on the plaintiff (Hasan I, 2011). Thus, the judge should ask the plaintiff to bring his witnesses or whatever evidence

to support his claim. In a case of an offence of extramarital sex relations (Zina), four adult sane pious males are required to give testimony, and two male adults in the event of the crime of murder (Hasan I, 2011).

However, the methods of proving the offence in Islamic law are a controversial issue because there are two points of view (AlKarmi 2005; Al-Zohaili 1994). The first point of view believes that these methods are limited to only the specific ways defined above; witnesses, confession and oath. These views are based on the Quran and the Sunnah (Al-Zohaili 1994). The second point of view believes that these methods are unlimited to include any method that leads to the truth which is called Qarinah (AlKarmi 2005; Al-Zohaili 1994).

4.4.5 Qarinah

The meaning of Qarinah in the Arabic language is a connection, conjunction, relation, union, affiliation, linkage or association. Legally, it refers to logical inferences to be drawn from circumstances. Besides that, it is also called a presumption, drawn from other facts proven or admitted to be true (Anwarullah, 2004). The majority of scholars from the leading four Islamic schools have accepted and recognised Al-Qarinah as one of the means of proof. There are three different views regarding this matter namely (Anwarullah, 2004):

1. The first view totally rejects the use of the Qarinah in both Hudud Hudud and Qisas crimes. This view is expressed by both Hanafi and Shafie's school.
2. The second view partially accepted Qarinah in determining Hudud offences about particular offences such as pregnancy of unmarried women, or smell of alcohol from the accused person (Anwarullah, 2004). Only Maliki's school is accepting this view (Al-Zohaili 1994).
3. The third view takes the most liberal way by recognising Qarinah in every case including Hudud Hudud and Qisas. According to Anwarullah, this group argued that evidence from the testimony of a witness is sometimes more susceptible to concoction and fabrication. As such, Qarinah may be seen as more compelling and stronger than the testimony of witnesses and confession because the real fact does not tell lies (Anwarullah, 2004).

Based on the last view, evidence could include the following (Anwarullah, 2004):

1. Circumstantial Evidence: is not evidence of the fact at issue, it is proof of the fact which can be used to infer information about the existence or non-existence of a fact in dispute.
2. Documentary Evidence refers to evidence of the contents of documents, including anything with information of any description recorded on it.
3. Original Evidence: depending on the context, it may refer to first-hand evidence or evidence which is not a result of a derivative process, such as an original handwritten document.
4. Real Evidence: the piece of evidence presented for examination to the finder of the fact, for example a knife covered in blood.
5. Hearsay: this is a statement made outside a court and produced as evidence in a court. For example, when person "A" has no direct knowledge about an event, condition or thing "E", but has gathered information pertaining to "E" from another person "B", then it is called hearsay if uttered by "A" in the court of law. Such information, if presented as evidence in a court, will be inadmissible. According to this definition, any out of court information becomes hearsay, thus in principle making digital evidence inadmissible to a court of law as it is not a direct knowledge, but an interpretation of reality. The law acknowledges this, and makes some exceptions for hearsay such as hearsay coming from a sufficiently reliable source, such as data produced or stored by a machine during its normal course of activity even without human involvement, which is deemed admissible.
6. Expert Evidence: The testimony of experts is defined as the testified opinion of a person with knowledge, expertise, skills, training or education, provided that their testimony is based on (i) sufficient facts and data, (ii) reliable principles and methods and (iii) their reliable application.

However, there are a number of rules for collecting evidence in Islamic law as follows (Al-Zohaili 1994):

a) It is based on scientific techniques: evidence should not be guessed or predicted but the evidence should be extracted from a scientific process;

b) It provides a link between a crime and its victim or a crime and its perpetrator. If there is a strong link between them this evidence is called strong otherwise it is weak evidence. Strong evidence is acceptable in Al-Sharia as a main method of proof in Sharia law; whereas weak evidence is unacceptable because it is based on prediction.

4.6 Forensic evidence

Forensic evidence today has become an integral part of civil litigation and crime investigation in Western jurisdictions. The history of forensic evidence has become an independent body since the 7th century in Europe. This led to the establishment of the Forensic Medicine Chair in Edinburgh UK, in 1807 (Haneef S, 2007). In the past 25 years, the forensic sciences have made dramatic scientific breakthroughs; DNA typing, physical evidence databases, and new scientific instrumentation (Peterson P, 2006). Computerised databases are another development that has changed the value of forensic science to the criminal justice system. Historically, and up until the mid-1980s, investigators needed a reference standard before they could make a statement of common origin. Latent fingerprints from a crime scene could not be used to identify an offender unless a known set of fingerprints could be obtained from one or more suspects. The manual filing systems in place were helpless in matching the latent print with the prints of their owner. Likewise, serologists needed a biological sample from a suspect before the source of blood or semen stain from a crime could be determined (Peterson P, 2006).

The four Islamic scholars (Hanafi, Maliki, Syafie and Hanbali) acknowledged that it is obligatory for the judges to rely on expert evaluation in complex cases which may require expert explanations to facilitate the judicial method (. This is proven based on a story where one of Prophet Mohammed's companions (Ali) had resolved a case in which a woman accused a young man that he raped her. She spread egg whites on her clothes and in between her thighs. The second Islamic leader Umar asked Ali to give his opinion in solving this case as an expert. Ali proved that the white patches were egg whites and not semen as alleged by the woman. Consequently, Islamic scholars have agreed on the importance of judges asking experts for help in solving the matters in which the courtroom is having a difficulty (Anwarullah, 2004). In Islam, expert opinion is only acceptable when it fulfils the conditions such those stated by the Islamic guideline from the Islamic Fiqh Academy for DNA tests. The expert is required to be a Muslim, sane, has reached puberty, an upright person and competent in his field. Furthermore, some scholars have raised other

requirements such as being able to see, hear and speak trustworthily, and the opinion should come from more than one expert (Al-Zuhailiy, 1994).

4.7 Digital Crime and Evidence in Islamic Law

The digital crimes laws under the Islamic code of ethics would open a discussion about digital crimes from an Islamic point of view and cover digital boundaries of computer operations, data communication for information access, transaction management and protection of economic and intellectual property (including physical, virtual and logical security of information and protection of infrastructure and equipment). Shariah law has the ability to envelop an entire spectrum in the cyber domain; i.e. individual vs. organizational, national and international (Anwarullah, 2004). Neither in the Quran nor in the Sunnah is mentioned the laws and penalties for digital crimes, but there are numerous relevant Quran verses and Sunnah covering these issues.

Protection against spying and breaking privacy

Entering into private or confidential files or other data without the permission of the owner on a PC or the network, or using the internet with bad intentions is not allowed. This data may be the property of an individual, organisation or data of national or international interest, which can be used against humanity or spreading terror in the society. Prophet Mohammad stated:

"Beware of suspicion, for suspicion is the greatest falsehood. do not try to find fault with one another, do not spy on one another, do not vie with one another, do not envy one another, do not be angry with one another, do not turn away from one another, and be servants of Allah, brothers to one another". In the Aya below we have an explicit prohibition not to spy on each other so the Quran determined the controversial issue.

(O ye who believe! Avoid suspicion as much (as possible): for suspicion in some cases is a sin: And spy not on each other behind their backs. Would any of you like to eat the flesh of his dead brother? Nay, ye would abhor it...But fear Allah: For Allah is Oft-Returning, Most Merciful)(Quran, Al-Hujurat: 12).

Protection of intellectual or binary property

Muslims believe that all property belongs to Allah. The private owner of property acts as a trustee or agent for Allah, the ultimate owner. Nevertheless, Islam cherishes the inviolability of private property (al-Zuhailiy, 1994). The Quran states, "And do not eat up your property among yourselves for vanities, nor use it as bait for the judges, with an intent that ye may eat up wrongfully and knowingly a little of (other) people's property" (Quran, al-Baqarah 2:188).

Prophet Muhammad in his farewell pilgrimage said; "No property of a Muslim is lawful to his brother except what he gives him from the goodness of his heart, so do not wrong yourselves". (Malkawi, 2013). Shariah thus takes a middle way between communal property rights and personal rights to property based on Western ideas.

Here is an example to provide further explanation: the process of software development is similar to manufacturing a tangible product (say furniture) because the producing unit (software-company) invested money, time and effort to develop such a product. There is an ownership of this product to someone. The use of other people's articles without their permission is not allowed - even strictly prohibited. Hence, the use of code, program or application, without the owner's permission is to be taken as stealing the virtual or intellectual property of others.

However, the bad effects are that society has been exposed to many illegal and immoral activities such as the commission of cybercrimes, degradation of moral values, social crises, the destruction of the marriage institution and insults on Islam. In fact, these cyber threats are the problems of today and the future which needed to be addressed in a comprehensive manner (Mohamed D, 2011).

Since the Quran allows Muslims to adopt any methods to prove a crime, it is clear the offence stands proven in Islamic law just like the worldwide acceptable methods of legal ethics authorized by logic and reason. Consequently, all the modern methods to prove evidence such as DNA testing and fingerprint are employed to ascertain a crime, and then this would be acceptable by Islamic law – the exception being with Hudud offences where only the testimony of witnesses, confession of criminals, or oaths are accepted.

4.8 Summary of chapter four

In Islamic law there are different types of punishments and different types of evidence accepted in the courtroom depending on the type of crime. Hudud punishments prescribed by God, such as flogging and exiling the unmarried adulterer, stoning the married adulterer, the punishment for highway robbery and flogging the imbiber of liquor. These crimes and their punishments are clearly stated in the Quran, where the judge cannot modify these punishments neither to reduce nor increase them. Moreover, these kinds of punishments can only be carried out on the basis of specific types of evidence such as; confession or the testimony of reliable witnesses since these punishments are God's right . The second type of punishment is retribution (Qisas), where the offender is punished with the same injury that he caused to the victim. For example, if the criminal killed the victim, then they should be killed if the family does not forgive them. Thirdly, the discretionary (Tazir) type of punishment is not fixed by Islamic law, which could be against the rights of God or the rights of a person. It is the broadest category of punishments, where the circumstances and evidence (Qarinah) are used as a method of proving or disproving.

The methods of proving offences in Islamic law are a controversial issue because there are two points of view (AlKarmi 2005; Al-Zohaili 1994). The first point of view believes that these methods are limited to only classical methods such as witnesses, confession and oath. These views are based on the Quran and the Sunnah (Al-Zohaili 1994). The second point of view is that these methods are unlimited to include any method that leads to the truth such as witness, confession, substantial evidence, bearing testimony (Al Qarinah) and a scientific method. The Quran allows Muslims to adopt any methods to prove a crime, and the four main Islamic scholars (Hanafi, Maliki, Syafie and Hanbali) acknowledged that it is obligatory for judges to rely on expert evaluations in complex cases. The majority of digital forensic investigations in Muslim countries have not understood the Islamic legal requirements for admissible evidence because their governments have only recently issued a law on combating cybercrimes. For example, Saudi Arabia issued the law in 2007, and the United Arab Emirates (UAE) issued their cybercrimes law in 2006. Formal controls in organisations are still not complete.

In summary, the Islamic religion is built on the relationship between an individual and God, which is moral, ethical and obliges a person to tell the truth in the court of law. Consequently, there is a conflict between the scientific and impersonal nature of the western legal system that is generated through scientific evidence, and the moral and religious obligation that is based on faith and trust of the Islamic religion. This chapter shows that there is a significant and interesting relationship between religion and digital evidence, which is worthwhile to study. Traditionalists believe that the law should be based on the religious traditional legal practice (testimony of witnesses, confession of criminals and oaths). The legal enforcement professional's perception of evidence could be affected by Islamic scholars' beliefs that modern evidence cannot be trusted. In this context, the potential research issues regarding the conflict between traditional and scientific legal practice have been identified but not resolved in the literature. These issues will be addressed by examining the role and the status of digital evidence in Saudi Arabian legal practice.

Chapter Five

THE ROLE AND STATUS OF DIGITAL EVIDENCE IN KSA LEGAL PRACTICE – ANALYTICAL FRAMEWORK AND RESEARCH METHODOLOGY

5.1 Introduction

In Section 5.2, quantitative and qualitative methods are introduced, primarily to explain the characteristics of both research methods. Furthermore, the section builds upon the relationship between both research methods while discussing the fundamental differences between the two and making a comparison of both in relation to this work. The argument is that qualitative research is most suitable for use in this thesis, as it aims to examine in what way and to what extent the Islamic religion and culture affect the status of digital evidence in the legal process from the perspectives of the legal practitioners involved in the entire process., It also examines the principles practitioners have to observe in the way they treat digital evidence in the judicial proceedings bearing in mind the differences between the traditionalist views based on religion and the digital forensic guidelines based on science. Finally, it assesses how digital forensic practitioners resolve this apparent conflict in practice.

In Section 5.3, the concept of triangulation is discussed – using more than one method to verify the same qualitative research. Triangulation is used as qualitative method as it is different from quantitative methods where there is numerical data to prove the correctness of its standpoint. The argument is that the concept of triangulation is a practical way to improve the credibility and trustworthiness of the results of the qualitative methods. This section expands on this and discusses the methods of triangulation; in particular the use of the literature survey, question survey, case studies and legal case review for this work. The sub-sections (5.3.1 – 5.3.4) give greater detail about the instruments that are used in this research, discussing the overall purpose, characteristics, advantages, disadvantages, procedures, limitations, and quality of these instruments.

Section 5.3.3 discusses the second method used in this research, which is case study, and outlines the definition, design, data sources, data collection, and quality of the case study performed.

Section 5.3.4 discusses the applicability of using law cases as a part of the triangulation. The use of law cases aims to obtain in-depth judicial opinions toward related cases and the actual decisions that the judges have taken.

Next, the methods used to ensure validity and reliability in this research are explained in section 5.5, followed by ethical considerations taken into account during this research.

5.2 Analytical Framework

The main aim of this chapter is to present the approach to the study of the influence of Islamic law and Saudi Arabian culture on the adoption of digital forensics in SA legal system. As shown in the studies of other cultures and religions (US, China, Jordan, Australia) discussed in detail in Chapter 2, religion and culture do have significant impact on different science in particular in the role of digital forensics in the legal process in those countries. In addition, chapter 2 significant aspects of Saudi Arabian culture and religion were discussed and specific areas identified where Saudi Arabian legal practice differs from the other cultures and societies. In particular, nepotism hierarchy, gender communication, fear of losing face, and favouritism influences the investigation since the officials responsible are not necessarily sufficiently qualified to handle the scientific detail involved in the preparation of digital evidence. The literature sources presented in chapter 2 confirm that Saudi Arabia is a religious country, where Islam provides the framework for the laws and government for its people. The Islamic religion is built on the relationship between an individual and God, which is moral, ethical and obliges a person, to tell the truth in a court of law, as discussed in chapter 3, since, in Islam it is generally accepted that traditional evidence, such a witness statements, confessions and oaths carry more weight in the courts of law.

For these reasons, the focus of the analytical framework developed in this study is on the role and status of digital evidence in the Saudi Arabian legal practice in comparison with

the traditional evidence. The use of digital evidence is new, requires a considerable degree of expertise in the fields of computer science, information technology, as well as familiarity with legal regulations and constraints. The nature of digital evidence is that is it non-intuitive, precise and every action can be traced and proved scientifically. For these reasons the value of digital evidence is different from the value of human witnesses. It is indeed, more difficult for the legal professionals (not trained in technology) to establish beyond any doubt that particular digital evidence is authentic and reliable, than to trust their own judgment based on legal education and experience.

What counts as a crime generally varies from society to society depending on cultures and religion, for example in Islamic societies any sort of female body exposure would be considered pornography. Similarly, slander, gambling, and abusing religionist-scholars are prohibited in Saudi Arabia, while it could be acceptable behaviour in some other societies as an aspect of personal freedom. Moreover, the type of legal punishment and the evidence found in an event of investigation differ from one society to another depending on religion and culture. These are serious issues specially when dealing with international electronic crimes, where the investigations crossing many borders on the way are complicated not only by evidence handling differences, but also by legal, religious, and cultural differences.

Therefore, it is important to follow the path of digital evidence from its discovery to the end of the legal process when innocence or quilt is established and sentences pronounced. It is also important to examine how digital evidence is treated throughout the entire legal process that is, in what way it is collected and analysed, presented to the court and regarded by the judges as a reliable proof of guilt or innocence of the defendants. A broad approach to engage all stakeholders involved is important in addressing the research question – that is - in what way and to what extent the Islamic religion and Saudi Arabian culture affect the status of digital evidence in the legal process. Therefore the focus of this study is to, examine the principles practitioners have to observe in the way they treat digital evidence in the judicial proceedings, especially how Islamic laws stand in respect to the admissibility of various kinds of digital data as evidence and how digital forensic practitioners follow this in practice. Saudi Arabia is an example of an Islamic country

practicing Islamic law as described in chapters 2 and 3 and it is expected that the findings of the study in Saudi Arabia can be generalized to other Islamic societies.

According to Mingers (2001), research results will be richer and more reliable if different research methods, preferably from different paradigms, are routinely combined. Therefore, triangulation of four methods would use to prove the credibility and reliable of the findings by using historical (literature) review, Survey, case interview and legal case reports which will be discussed in next section.

5.3 Methodology

The use of a proven and reliable research methodology is a vital component of research; it is the only means of producing reliable outcomes in the work produced. The aim of this chapter is to discuss the most effective methods to answer the research questions. In addition, this chapter introduces the differences between quantitative research and qualitative research, and gives explanations of quality measurements that are applicable to this research.

5.3.1 Quantitative and qualitative methods

The use of a proven and reliable research methodology is a vital component of research; it is the only means of producing reliable outcomes in the work produced. This chapter aims to discuss the research methodology used for this work, as a means of finding the most useful way of answering the research questions posed. This chapter will not only discuss the differences between research methodologies (quantitative and qualitative research), but also presents the explanations of quality measurements, such as validity and reliability, that are applicable to this research.

Hughes and Cotterell (2002) declare that methodologies and methods are rather confused and overlapped terms; however, “methodology is the set of methods that are used on a project”. Methodology is studying methods and arguments about philosophical theories of the research process; whereas, method is an exact procedure of data collection

concerning these philosophical theories. There are two wide methodological approaches; the logical and the empirical positivism. Based on these methodological approaches, we are lead to the two main research methods: quantitative and the qualitative.

5.3.1 Quantitative method

The quantitative method is defined by Aliaga and Gunderson (2000) as "Explaining phenomena by collecting numerical data that are analysed using mathematically based methods (in particular statistics)". From this definition, we understand that quantitative research is research that uses numerical analysis. In essence, this approach reduces data into numbers, so it is designed for collecting data for statistical analysis and is mostly linked with experiments and questionnaires. It is related with *antipositivism* that rejects the scientific approach, *hermeneutics* that attempts to interpret and *phenomenology* that studies the event.

5.3.2. Qualitative method

The qualitative method relies on observation and unstructured interviews. It is actually called so in order to distinguish it from quantitative methods. (Wilson, 1999), define qualitative research as a, "…multi-method in focus, involving an interpretive, naturalistic approach to its subject matter. This means that qualitative researchers study things in their natural settings, attempting to make sense of or interpret phenomena in terms of the meanings people bring to them. Qualitative research involves the studied use and collection of a variety of empirical materials - case study, personal experience, introspective, life story, interview, observational, historical, interactional, and visual texts - that describe routine and problematic moments and meaning in individuals' lives". Marshall (2006) concludes that qualitative research typically relies on four methods for gathering information; participating in the setting, observing directly, in-depth interviewing and analysing documents and material culture. The ways of qualitative data collection cover interview, questionnaire and observation.

Firstly, qualitative content analysis of interview data aims to describe every stage and target (in this particular case diabetes was being studied). Lundman & Norberg (1993) studied that their unit of analysis is interview text about experiences of having hypoglycaemia, and the context consists of a larger study aimed at describing coping strategies related to the everyday strains of living with diabetes. Graneheim & Lundman (2004) pointed out that the key point of data analysis in interviews is to compare the differences and similarities between the various codes and sort them into different sub-categories or categories, which has been identified before and helps to make manifest content.

Secondly, the data in observation is from notes and dialogues. As for the context in observations, Graneheim et al. (2001) state that it aims to illuminate the noted behaviours, called, 'behavioural disturbances'. In order to analyse the qualitative data in observation, the first step is to divide the observational notes and dialogues into several meaning units. This effectively helps us to get results from this data.

Thirdly, questionnaires or surveys will be used to collect enough data from the subjects. Even though the number of respondents to questionnaires is usually bigger than that of interviews, the scale is not big enough with the questionnaire in the quantitative approach. Elo & Kynagas (2007), defined sample is "studied the process, selecting the unit of analysis, making sense of the data and the whole, open coding, coding sheets, grouping, categorization and abstraction in inductive research; develop structured analysis matrices, data coding according the categories and hypothesis testing correspondence comparison to earlier studies etc. in deductive research.

This is the major reason why the qualitative method is adopted in this research, as this study seeks to find out the impact of religion and culture in digital investigations and the legal enforcement professional attitudes toward digital evidence in Saudi Arabia.

Surveys and case study interviews are the methods commonly used in qualitative research and its scope is an experimental method that investigates uptodate phenomenon within its real-life context; when the boundaries between phenomenon and context are not

clearly evident; and in which multiple sources of evidence are used (Feagin et al, 1991). Schramm (1971:page?) expressed the meaning of case study as, "…that it tries to illuminate a decision or set of decisions: why they were taken, how they were implemented, and with what result." Moreover, Feagin et al (1991:page?) stated that, "The quintessential characteristic of case studies is that they strive towards a holistic understanding of cultural systems of action."

5.4. Triangulation

Triangulation is, “The protocols that are used to ensure accuracy and alternative explanations...” (Ragin, 1989). Mathison (1988) pointed out the importance of triangulation, and noted that , “Triangulation has risen as an important methodological issue in naturalistic and qualitative approaches to evaluation (in order to) control bias and establishing valid propositions because traditional scientific techniques are incompatible with this alternate epistemology”. Mingers (2001) is another scholar who supports the theory of triangulation; he states that, “…research results will be richer and more reliable if different research methods, preferably from different (existing) paradigms, are routinely combined”. Amaratunga and Baldry (2001), define four types of triangulation, and they are:

1. Data source triangulation: “When the researcher views for the data to remain the same in difference contexts”.
2. Investigator triangulation: “When many investigators examine the same phenomenon”.
3. Theory triangulation: “When investigators with different viewpoints interpret the same result”.
4. Methodological triangulation: “When one procedure is followed by another, to increase confidence in the interpretation.”

The need for triangulation is usually necessary for qualitative research since qualitative research normally does not have numerical data or statistical information to prove and to support the accuracy of its findings. Thus, more than one systematic analysis method gives qualitative researchers the ability to prove and to claim the robustness of the findings. This shows that triangulation means that different research methods use different techniques to analyse the same problem from various angles. From this, practitioners of qualitative research can claim that these findings are ‘accurate’. Based on the previous discussions, it is understood that the concept of triangulation plays an important role in qualitative

research. Some current works which use the concept of triangulation include Amaratunga and Baldry (2001). It has been proven that triangulation can improve the quality (credibility) of qualitative research (Patton, 1990). Furthermore, Denzin, N. K., and Lincoln (1994) agree that once the credibility of qualitative research is ensured, it means the dependability of qualitative research is confirmed as well. Therefore, in this research, three research methods will be used to follow the concept of triangulation and to prove the credibility of the findings of this research. To get a reliable result a historical (literature) review, survey, case study and legal case reports were used as research methods.

5.4.1 Literature search

The literature is searched for content pertaining to the subject of the research. A careful search was conducted of both national and international literature including books, journal articles, course material, theses and dissertations, government publications, laws/statutes, encyclopaedias and literature found on the internet. The literature will serve as guidelines in obtaining relevant answers for this research. As the goal of this research is to examine in what way and to what extent do culture and religion affect the status of digital evidence in the legal process, the literature will therefore review and highlight how culture and religions play a role in different sciences, in particular ICT (Denzin, N. K., and Lincoln, 1994). Furthermore, it will examine cultural factors influence the status of legal processes, and how the existing Islamic laws favour the admissibility of various kinds of digital data as evidence. Finally, it finds out to what extent judges likely to recognize different kinds of digital evidence.

Furthermore, a review and examination of the existing procedures and guidelines in Western countries, which served to identify the principles the practitioners have to observe in the way they treat digital evidence in the legal process, will be conducted. This will undoubtedly provide a framework for Saudi Arabia for law enforcement practices and public prosecutors.

There was little written literature from the Islamic perspective, which is specific to the research questions posed in this thesis. In contrast, there was a reasonable number of international sources that were relevant to this research.

5.4.2 Survey method

5.4.2.1 Overview

A survey is any activity that collects information in an organised and methodical manner about characteristics of interest from some or all units of a population using well-defined concepts, methods and procedures, and compiles such information into a useful summary form (Ivan P, 2010). A survey usually begins with the need for information where no data – or insufficient data – exist.

Newsted *et al* (1998) state, "A survey is a way of going from observations to theory validation." Accordingly, it is correct for this research to use survey methods to interpret the noted observations. Newsted *et al* (1997) stated that, "In an interpretivist context surveys are appropriate as a complement to other forms of data or observations. They can serve as a way to add to one's knowledge through "triangulation" as one of several methods. Thus it is important to realize that while surveys are typically used in quantitative research, they can also help qualitative researchers as well." The survey instrument method will be used as a good method of collecting data as described by Linstone and Turoff (2002). They stated that, "the individuals needed to contribute to the examination of a broad or complex problem have no history of adequate communication and may represent diverse backgrounds with respect to experience or expertise." Linstone and Turoff (1975) gave a view of the survey method as being, "characterized as a method for structuring a group communication process, so that the process is effective in allowing a group of individuals, as a whole, to deal with complex problem." (Linstone, H, 1975). Furthermore, there are other researchers who agree that the survey technique is appropriate for qualitative research (Woudenberg, 1991).

Ali (2005) stated that the strengths of the survey technique outweigh its limitations; he provided seven suggestions to reduce problems caused by conducting a survey:

1. Using broad questions in the first round of a survey may discourage experts with time constraints to participate in a study, which was indicated by the drop out of some participants in the first survey study accommodate. Less broad survey questions should be considered to stimulate expert participation in a survey study.

2. The time scheduled to conduct a survey study should be flexible to conflicting schedules of participants, and give participants sufficient time to think and rethink about issues of concern without time pressures.

3. Follow-ups are critical to have prompt responses to survey rounds. A researcher should not be discouraged by low response rates to survey rounds. Instead, he/she should find ways to seek more participation by sending follow-ups for each round until a required rate of response is reached.

4. Providing incentives (e.g. monetary, certificates of appreciation from a major institution, and gifts) to contributors to a survey study will encourage more experts to participate and respond promptly to Delphi round questionnaires.

5. Using e-mail or e- form to conduct a survey is effective, fast, and cheap, but technical communication problems in many countries, especially the developing one.

6. Adopting majority voting as a means to analyse responses to survey rounds would produce reliable findings and demonstrate controversial issues, especially in large panels.

7. Categorizing responses to Delphi survey (e.g. legal authority, relative autonomy, levels of control, and capacity) enabled the researcher to summarize responses to round questionnaires. That can help the analyst summarize responses to survey rounds when participants have diverse expertise and provide a wide range of valid responses.

In this study, the survey method will be used to collect opinions from experts involved in digital forensics in Saudi Arabia. The objective of using a survey in this study is to evaluate and examine in what way and to what extent Saudi culture and the Islamic religion affect the legal process in investigating digital crimes? As such, the survey will

determine the current situation within the field of digital forensics in Saudi Arabia. Its aim is also to find out the level of education and certifications of those involved in digital forensics and assess the attitudes of legal enforcement members toward digital evidence.

5.4.2.2 Panel size

When choosing participants for completing the survey, the most important factor was the expertise and experience of the chosen digital forensic experts - in order for them to be able to provide valuable opinions. In this thesis, we will invite a number of digital forensic experts from Saudi Arabia to participate in the survey. The number of expert members involved in legal enforcement in digital forensics is relatively limited, especially in Saudi Arabia. Due to this reason, digital investigators, legal advisers, academic experts and judges were included in this study alongside digital forensic professionals. However, generally speaking, it is much better to get a high reply rate from a random, small sample rather than a low response rate from a big pool of possible respondents. According to D. Nulty (2008), surveys that are distributed internally (i.e. to employees) generally have a much higher response rate 30-40% than those distributed to external audiences 10-15%). To overcome the limited number of experts involved in digital forensics, we designed an e-survey and sent it to experts using three ways:

1. Internal distribution: through the training and development department in the Bureau of Investigation and Public Prosecution;
2. Direct contact: academic members and PhD students involved in legal enforcement procedures in digital forensics;
3. Saudi Cultural Bureau Recommendation: digital investigators, legal advisers and judges.

The choice of participants in a survey can greatly affect the outcome of the process, and therefore the choice of participants is very important. Due to the uniqueness of the

digital forensics profession, participants were chosen after careful consideration of their professional backgrounds.

There are numerous academic sources that discuss the size of a panel required to achieve a reasonable outcome within a survey. Different researchers have different thoughts on the numbers of respondents required for a survey based research, and there is no strict number of required participants (Fitch et al 2001). The size of a panel is changeable for a survey process, but the experts have similar backgrounds groups of ten to twenty participants might be enough (Clayton, 1997).

Based on the above discussions, it is apparent that there is no regulation for the size of a participant pool when using surveys. Consequently, an electronic survey using Google surveys was sent to 30 experts with different backgrounds for their participation. This is due to the number of experts in the field of digital forensics being limited. Furthermore, the decision is not going to affect the effectiveness of the survey in this research due to the results found by Clayton (1997) and Fitch et al (2001).

5.4.2.3 Questions design

As discussed earlier, creating surveys consist of several interconnected steps which include: defining the objectives, selecting a survey frame, determining the sample design, designing the questionnaire, collecting and processing the data, analysing and disseminating the data and documenting the survey. The life of a questionnaire design can be broken down into several phases. The first is the determining the questions to be asked in the planning phase, which is followed by selecting the question type for each question and specifying the wording. The final step consists of designing the question sequence and overall questionnaire layout.

Boddington (2008) stated in his review, "validating digital evidence for legal arguments" is now common in legal cases, but the understanding in the legal fraternity as to how far conventional ideas of evidence can be extended to the digital domain lags

behind. Evidence determines the truth of an issue but its weight is subject to examination and verification through existing forms of legal arguments. There is a need for a practical 'roadmap' that can guide the legal practitioner in identifying digital evidence which is relevant in supporting a case and assessing its weight. A vital but sometimes underestimated stage is that of validating the evidence before evaluating its weight (Boddington R, 2008). For the legal practitioner, research has attempted to enhance analysis of the weight of evidence as part of structuring legal arguments, but with limited adoptions to such processes (Tillers, 2005). Computer and network security and digital forensics research provides documentation about the properties of digital evidence but it does not explain it in a legal context which is helpful to the legal practitioner (Spenceley, 2003). The validation and acceptance of the evidence, however, is largely differing from one culture to another. Validation and acceptance of the evidence depends on four main factors:

1. Professional education and certification in the field of digital forensics,
2. Roadmap and policy,
3. Understanding legal issues and the members of the court to understand digital forensic issues,
4. Good practice and attitudes during the investigation process.

These four factors could be used as the main dimensions to understand and answer the research questions which are as following:

1. In what way and to what extent do culture and religion affect the status of digital evidence in the legal process?
2. What principles do the practitioners have to observe in the way they treat digital evidence in the legal process?
3. How do Islamic laws stand in respect to the admissibility of various kinds of digital data as evidence?

4. What are the principles that the practitioners have to observe in the way they treat digital evidence in the legal process for law enforcement practices and public prosecutors in Saudi Arabia?

Consequently, four dimensions and a total of twenty-eight different questions were designed.

Current situation and personal skill dimension:

Developing legal arguments can be frustrating if unskilled use is made of digital evidence, with unanticipated and often detrimental outcomes. For example, when presenting a legal case based on what appears to be convincing digital evidence, the case can collapse if the defence can show that the security integrity of the network is defective and shows contamination or alteration of the digital evidence it is supposed to protect. Therefore, if the validity of the evidence can be established, its weight in legal argument is enhanced. However, if its validity is uncertain or invalidated, then the weight of the evidence is diminished or negated (Boddington R, 2008). The aim of this dimension is to determine the current situation within the field of digital forensics and to find out experts' attitudes toward the skills of digital forensic.

Education and certification dimension:

Few legal practitioners have the sufficient technical expertise to analyse digital evidence in case preparation and it is difficult for them to present it in simple comprehensible terms to judges and juries; what may seem a potentially successful case based on straightforward legal argument can turn into a needless failure (Yasinsac et al, 2003). The aim of this dimension is to find out if there exist certifications for computer forensic experts and organizations with regards to training and education in the field of digital forensics.

Policy and organization dimension:

All governments and organizations should have standards, policies and procedures in place that can assist in an investigation. These governments and organizations should also have legislative measures that support organizations attempting to prosecute digital crimes. In 2001, The Digital Forensic Research Workshop (DFRWS) identified a seven step process namely, identification, preservation, collection, examination, analysis, presentation, and decision. In 2008, the U.S. Department of Justice (DOJ) released 'Forensic Examination of Digital Evidence: A Guide for Law Enforcement'. In 2012, the 'Good Practice Guide for Computer-Based Electronic Evidence' was provided by the ACPO, which is the UK standard that provides the procedure that should be followed by practitioners and focuses on the collection of evidence. The aim of this dimension is to find out Saudi Arabian national interaction between digital forensics and security organizations, and to determine if digital readiness is a popular policy for government organizations or private companies.

Law dimension:

Judges decide what evidence will or will not be allowed in their courtrooms. As a consequence, in evaluating scientific and technical evidence, judges must make informed decisions about the admissibility of such evidence at trial (Wegman, 2005). In addition, judges must determine the acceptability of expert witnesses who might testify about scientific and technical issues (Ball, 2008). The aim of this dimension is to understand how members of the court consider digital forensics and legal issues.

5.3.2.4. Survey procedures

The following six steps show the whole process of producing the survey:

First step: Selecting the participants

This step is to make sure that only experts who are involved in the digital forensics process participate. The backgrounds of these experts must be carefully evaluated. However, it

allows a greater variety of opinions and thoughts to choose experts for participation with different backgrounds (e.g. practitioners, academic, lawyers, and judges).

Second step: Choosing questions

The aim of this stage is to ask the respondents to choose the qualified and suitable questions. This was discussed in more detail in section 5.3.2.3

Third step: First round questionnaire

Since the questions are obtained from preceding literature and created independently, all the questions are further checked and reviewed by two digital forensic experts from the UK and one from Saudi Arabia. This is a very important step to assure the good quality of the questions.

Fourth step: Pilot test

Even the expert survey designer might write a survey which looks understandable, but could be confusing to the participants. Testing the survey before implementing it will help to obtain better data and useful information (Suskie, L. A, 1996). Therefore, the aim of this step is to make sure that the participants understand the survey correctly, through asking three participants to take part in the survey and give their feedback. The responses were then reviewed carefully looking for any inconsistencies or unexpected answers. Next, we made all necessary changes to the survey before implementing it.

Fifth Step: Sending the surveys

The choice of participants in a survey can greatly affect the outcome of the process, and therefore the choice of participants is very important. To make sure a good number of experts involved in digital forensics participated in this study, we designed an e-survey and sent it using three ways:

1. Internal distribution: Through the training and development department in the Bureau of Investigation and Public Prosecution;

2. Direct contact: Academic members and PhD students involved in legal enforcement procedures in digital forensics;
3. Saudi Cultural Bureau Recommendation: Digital investigators, legal advisers and judges.

Sixth step: Analysing the feedback

The aim of this step is to analyse and interpret the answers, data and information provided by respondents. This step enabled us to produce particular insight for this research, which is the contribution of this technique in this research.

5.4.3. Case interview

According to Yin (1989), "The case study contributes uniquely to our knowledge of individual, organizational, social, and political phenomena", and, "The unique strength is its ability to deal with a full variety of evidence –documents, artefacts, interviews, and observations. Moreover, in some situations, such as participant observation, informal manipulation can occur". Also, Tellis (1997: page?) notes that "Case studies are designed to bring out the details from the viewpoint of the participants using multiple sources of data".

The five components designed by Yin (1994) are of particularly significant importance for new case study researchers as it will enable them to build good case studies individually. The five components are as follows:

1. A study's questions (*who*, *what*, *where*, *how*, and *why*);
2. Its propositions (pinpoint the issues which should be explored in the study)
3. Its unit(s) of analysis,
4. The logic linking the data to the propositions; and
5. The criteria for interpreting the findings.

Yin (1989) stated that there are at least six different sources that could be used in a case study to aid in the reliability of the research. They are: documentation, archival records, interviews, direct observation, participant observation, and physical artefacts. These six different data sources have their unique characteristics, and on the other hand, have typical weaknesses as shown in table .1 (Yin, 1994).

Table .3: Different Data Sources Advantages and Disadvantages

Source of Evidence	**Advantage**	**Disadvantage**
Documentation	1. Stable: repeated review 2. Unobtrusive: exist prior to case study 3. Exact: names etc. 4. Broad Coverage: 5. extended time span	1. Retrievability: difficult 2. Biased selectivity 3. Reporting bias: reflects 4. author bias 5. Access: may be blocked
Archival Record	1. Same as above 2. Precise and quantitative	1. Same as above 2. Privacy might inhibit access
Interview	1. Targeted: focuses on case study topic 2. Insightful: provides perceived causal inferences	1. Bias due to poor questions 2. Response bias 3. Incomplete recollection 4. Reflexivity: interviewee expresses what interviewer wants to hear
Direct Observation	1. Reality: covers events in real time 2. Contextual: covers event context	1. Time consuming 2. Selectivity: might miss facts 3. Reflexivity: observer's presence might cause change 4. Cost: observers need time
Participant	1. Same as above	1. Same as above

Observation	2. Insightful into interpersonal behaviour	2. Bias due to investigator's actions
Physical Artefact	1. Insightful into cultural features 2. Insightful into technical operations	1. Selectivity 2. Availability

The only way to mitigate the disadvantages of each is to use multiple sources, so that they will be used in conjunction with other research methodologies.

The use of case study along with the other methods is an important instrument in this study, as it is one possible research methodology used to collect multiple sources of evidence to answer the research questions. The meaning of and reasoning behind the need for a case study database can be found in Yin (1989) as he stated, "Every case study project should strive to develop a formal, retrievable database, so that in principle, other investigators can review the evidence directly and not be limited to the written reports. In this manner, the database will increase markedly the reliability of the entire case study."

5.4.3.1 Data Collection of Case Study

As discussed above, data collection methods being used as part of the case study methodology is an important component of the method. The main benefit of interviewer-assisted methods is that by personalising the interview and being able to interpret questions and survey concepts, the interviewer can increase the response rate and overall quality of the data. Interviewer-assisted methods are particularly useful for survey populations with low literacy rates or when the concepts or the questionnaire are complex, or anytime self-enumeration would be difficult. Also, the overall quality of the data can be improved if the interviewer has good knowledge of the survey's concepts, aims and objectives which will help respondents with any problems interpreting the questionnaire. The interviewer can

prevent response errors and item non-response by immediately identifying errors and correcting them in the presence of the respondent. This also reduces follow-up which can be time-consuming for the survey agency and burdensome to the respondent. Another advantage of interviewing is that it allows for more flexible collection periods: if data collection is going too slowly and needs to be accelerated. This is not possible with self-enumeration methods where there is little control over when the respondent completes and returns the questionnaire.

5.4.3.2 Quality of the case study

This research introduces the different backgrounds of interview respondents to demonstrate that they are experts in field of digital forensics. The approach used in this research is to invite a broad range of legal professionals involved with digital forensic approaches to participate in the case study interviews in order to satisfy the data source triangulation. The twelve experts include; three legal investigators, four lawyers, three academics and two judges. The sources of these interviews helped to reaffirm the concept of data triangulation, which also confirms the validity and credibility of the case study. The experts chosen to participate in the case study have practical backgrounds and legitimate experiences of the legal enforcement process of collecting, analysing and presenting digital evidence in the event of digital crime. The participants must have a thorough knowledge of the current situation within the field of digital forensics and the legal system in Saudi Arabia. Consequently, digital forensic practitioners, academics, lawyers, and judges are eligible and suitable to participate. With such a broad range of legal professionals involved with digital forensic approaches taking part in the study, it ensures the credibility, transferability, and dependability of the answers. Moreover, case studies, unlike surveys, seek in-depth answers about digital forensic situations. According to Neuman (1997) and Sarantakos (1998), reliability tells us about an indicator's dependability and consistency throughout the research process, i.e. the degree to which it can be repeated. Also, Custer, (1999 page?) stated, "The validity of the modified survey process depends on the careful and systematic application of procedures for initial competency selection (e.g. reviewing

the literature, developing a table of specifications, and conducting a pilot test)". In this work we ensured this by following the scientific methods for methods design.

Whilst a single instrument might have disadvantages and limitations, the purpose of using multiple sources of evidence was to comply with the standard of data source triangulation. Furthermore, using multiple data sources can address the problem of construct validity, and reliability, since multiple data sources use different evidence to describe and to prove the same phenomenon.

5.4.3.3 Quality of Questions

The questionnaire for the case study was built using the two steps to be used in the survey; literature and asking three experts to check the quality of the questionnaire. In addition, the third step was used the outcome of the survey review and answers provided by the participants. Consequently, using multiple data sources in these cases enabled an in-depth evaluation of the situation of digital forensics in Saudi Arabia. Similar in nature to the design of the survey questionnaire, the case study interviews used the same dimensions. The dimensions were used as baselines to assess the current digital forensic situation in Saudi Arabia. There are thirteen different questions in the case study questionnaire, and the full questionnaire.

5.5.4 Legal case review

Case law is the collection of reported cases that form the body of law within a given jurisdiction. It is based upon judicial opinions by various courts, which may set future precedent.

Judicial opinions (also known as legal opinions, legal decisions, or cases) are written decisions authored by judges explaining how they resolved a particular legal dispute and explaining their reasoning. An opinion tells the story of the case: what the case is about, how the court is resolving the case, and why.

The advantage of using law case study is to help understand the law and the actual decisions that the judges have taken - understanding the way that judges look at law. More importantly, it shows a real case and disputes because real cases and disputes have historically been the primary source of law. In addition, this helps in:

1. Determining the constitutionality of a proposed act or policy (often in response to a request by one of the other branches government);
2. Determining the law governing a case before a court in a different jurisdiction where the jurisprudence available is considered inadequate to dispose of the questions the case presents;
3. Defining how government rules and regulations are intended to be administered.

5.6 Methods to ensure validity and reliability

One of the major concerns with any research is to ensure that the research quality and validity are high. Validity concerns the accuracy of the questions asked, the data collected and the explanation offered. It relates to the data and the analysis used in research (Denscombe, 2002). The researcher ensured that the data collected was valid by consulting books, journals, periodicals, and information from the internet which was relevant to the aims and research questions of the research. According to Neuman (1997) and Sarantakos (1998), reliability tells us about an indicator's dependability and consistency throughout the research process, that is, the degree to which it can be repeated. To ensure reliability, we should make certain that if the same methods are used by different researchers and/or at different times, they should still produce similar results.

Within the survey instrument, this is no exception. Custer et al (1999) state that, "The validity of the modified survey process depends on the careful and systematic application of procedures for initial competency selection (e.g. reviewing the literature, developing a table of specifications, and conducting a pilot test)". In this work, we ensured that the scientific methods and survey design are properly used. Also, as discussed in the above

section, in this research, we will adopt the concept of data source triangulation in order to promote validity. Although a survey instrument on its own may have disadvantages and limitations, they can be surmounted with the production of a high quality survey and with the use of other research methodologies used to support the findings and outcomes. The purpose of using multiple sources of evidence within a case study is to comply with the standard of data source triangulation. Furthermore, using multiple data sources can address the problems of construct validity and reliability, since multiple data sources use different evidence to describe and to prove the same phenomenon.

The justification for a case study database can be found in Yin (1989) who states that "Every case study project should strive to develop a formal, retrievable database, so that in principle, other investigators can review the evidence directly and not be limited to the written reports. In this manner, the database will increase markedly the reliability of the entire case study." Therefore, the interviews will be considered valid since we will interview experts with general knowledge about digital evidence, using an interview schedule based on the research aims and questions. All of these factors ensure that the instrument measures what it is supposed to measure. The data will beanalyzed using an appropriate data analysis method in order to ensure validity as stated by Leedy and Ormrod (2005). Equally, the triangulation approach which will be used, will further strengthen the trustworthiness of the data obtained.

5.7 Scope of the study

Since the aim of this study is to determine the impact of culture and religion on the role and status of digital evidence in legal practice, using Saudi Arabia as an example of Islamic country practising Islamic law. Also, an aim is to determine the current situation of the Saudi Arabia criminal procedure and identify the differences between Saudi Arabia legal enforcement procedure and ACPO-guided procedure used in the UK. Moreover, the expected outcome is to identify the principles that the practitioners have to observe in the way they treat digital evidence in the legal process in Saudi Arabia and Islamic countries.

Therefore, the approach used in this research was to invite a broad range of Saudi

professionals involved with digital forensic investigations, legal analysis and research to participate in the study. This approach helped to overcome the limited number of digital forensic investigators in Saudi Arabia in particular. Furthermore, it provided more credibi and reliable approach, since surveying the whole spectrum of the legal enforcement gives clearer understanding of the current situation of the Saudi Arabia criminal procedure and of the principles that practitioners have to observe in the way they treat digital evidence.

The experts chosen to participate in the case study have practical backgrounds and extensive experience in the legal enforcement process to collect, analyse and or present digital evidence in the event of digital crime. Consequently, the digital forensic practitioners, academics, lawyers, and judges were eligible and suitable to be involved in this study. These data helped to develop a novel analytical framework built upon in-depth understanding of the current situation in Saudi Arabia, ACPO and number of existing digital forensic frameworks, in addition to International Islamic Fiqh Academy (IIFA) recommendations for modern evidence such as e-contract and DNA fingerprinting.

Furthermore, legal cases used to investigate legal procedures in Saudi Arabia in case of digital crimes, particularly from the standpoint of analyzing the gaps in the existing legislation that could have held back the prosecution of the offending parties. All the three cases were collected from Government official sites, the first case was presented in the site of the Ministry of Justice and the other two cases were presented at the Communication and Information Technology Commission.

5.8 Summary of this chapter

The purpose of this chapter is to discuss the role and status of digital evidence in Saudi Arabia legal practice – analytical framework and research to answer the research questions. In addition, this section introduces the differences between quantitative research and qualitative research, and gives explanations of quality measurements that are applicable to this research. Moreover, shows that research results will be richer and more reliable if

different research methods, preferably from different paradigms, are routinely combined (Mingers, 2001). The need for triangulation is usually necessary for qualitative research since a qualitative research normally does not have numerical data or statistic information to prove and to support the accuracy of its findings (Mingers, 2001). Thus, more than one systematic analysis method gives the qualitative researchers ability to prove and to claim the robustness of the findings. Therefore, to get a reliable result historical (literature) review, survey, case study and legal case reports are used.

The literature served as guidelines in obtaining relevant data which not only illustrates the relationship between culture, and different sciences, but also shows that there is a significant and interesting issue between culture, religion and digital evidence, which is worthwhile to study.

While, the survey method used to collect opinions from experts involved in digital forensic in Saudi Arabia. There are numerous academic sources discussed the size of a panel required to achieve a reasonable outcome within a survey. Different academic researchers have different thoughts on the numbers of respondents required for survey based research, and there is no strict number of required participants (Clayton 1997; Fitch et al 2001). The size of a panel is changeable for a survey process, but with experts have similar backgrounds group of ten to twenty participants might be enough (Delbecq et al, 986; Delbecq et al, 1986; Clayton, 1997). Based on this, electronic survey designed using Google survey and sent to 30 experts but only 13 responded. For more reliable results, case study interview used to seek in-depth answers of digital forensic from the experts where the overall quality of the data can be improved as the interviewer has good knowledge on the survey's concepts, aims and objectives which will help in respondent with any problems interpreting the questionnaire. This research introduces the different backgrounds of interview respondents to demonstrate that they are experts in field of digital forensics. The approach used is inviting broad range of legal professionals involved with digital forensic approaches to participate in the case study interviews so as to satisfy the data source triangulation. The eight experts include; 3 legal investigators, 2 lawyer, 1 academic and 2 Judges. Consequently, the digital forensic practitioners, academics, lawyers, and

Judges are eligible and suitable to do this job. Such broad range of legal professionals involved with digital forensic approaches, assure the credibility, transferability, and dependability of the answers. While, the purpose of using law cases in this study was to know the legal procedure used in searching, collecting, seizure and analysing digital evidence. Furthermore, it provides actual information about the existing gaps in the legislations and the judicial opinions toward the offence. All the three legal cases where collected from Government official sites, the first case was presented in the site of Ministry of Justus and the other two cases were presented on Communication and Information Technology Commission.

The entire digital forensic process, from collecting digital evidence to its influence in arriving at judgment and sentencing would be investigated through. The respective roles of different agencies, the police, the forensic analysts, the defence and the prosecuting lawyers, the judges and the courts, are also taken into account. The nature of the interactions between these agencies, as well as the integrity of the information and evidence throughout the legal process would be examined.

Chapter Six

FINDINGS AND DISCUSSION

6.1 Findings

6.1.1 Findings of Survey

6.1.1.1 Current Situation and Personal Skill Dimension

Methods of proving the offence in Islamic law is a controversial issue because there are two points of view (AlKarmi 2005; Al-Zohaili 1994). The first point of view believes that these methods are limited to only classic methods such as witnesses, confession and oath. These views are based on the Quran and the Sunna (Al-Zohaili 1994). The second point of view believes that these methods are unlimited to include any method that leads to the truth such as witness, confession, substantial evidence, bearing testimony (Al Qarinah) and scientific methods.

The aim of this dimension is to determine the current situation within the field of digital forensics and personal skill, to better our understanding and develop baselines from which further conclusions may be drawn. The details of this stage of data collection and discovery methods are presented in Appendix 1 and 2. However, Seven participants including three academic researchers, two computer scientist and two officers agreed that there is no well-established organisation for digital forensic in Saudi Arabia. However, all the participants agreed that Saudi Arabia government does understand the importance of digital forensics, and there are real efforts to improve this important field. The only exception is that academics stated that Saudi Arabia government does not put enough weight on digital forensics developments. However, the other participants indicated that the development of digital forensics would be improved shortly. Also, respondents agreed digital forensics is not a topical subject in Saudi Arabia in general, but it is an important topic in legal enforcement against terrorism. Consequently, Saudi Arabia government starts to give more attention towards forensics following the fast growth in this field. Moreover, seven participants further indicated that organisations involved in digital

security and forensic are cooperate with each other, while the other five participants believed there is no good cooperation between these organisations. This is an important issue where investigated further in case interview. In addition the participants stated that there are shortage of staff in digital forensic filed but not explained why the numbers of specialists are limited. These finding findings identify the current situation within the field of digital forensics but still leave some gaps need to be clarified more in case interview.

6.1.1.2 Education and certification Dimension

Few legal practitioners have sufficient technical expertise to analyse digital evidence in case preparation: it is difficult for them to present it in simple, comprehensible terms to judges and juries. What may seem a potentially successful case based on a straightforward legal argument can turn into a needless failure (Yasinsac et al, 2003). The aim of this dimension is to discover if there exist certifications for computer forensic experts, and organisations regarding training and education in the field of digital forensics. The details of this part of the investigation are presented in Appendix 2. However, all participants stated that the there is no specific qualification required to work in Digital Forensic as far as it is one of the following qualifications: computer science, Law, Policing and Criminology. Two academics give the two explanations behind it, first one the field at its early stage in Saudi Arabia. Secondly, there is a significant shortage of specialist to cover the rapid growth of digital uses and its associated illegal issues. This is critical point was discussed in more ditties in the case interview. Moreover, two-third of the participants stated that both qualification and experience are required. On the other hand, participants stated that the Saudi Arabia government is fully supporting education and training in the field of digital security and forensics. Similarly, nine participants agreed that there is no particular institute to certify the qualification of digital forensic practitioners. Moreover, the participants agree there is no well organised on-the-job training for digital forensic investigators.

This dimension indicates that Saudi Arabia government understand the importance of digital forensic and the field not perfect at this stage and there is much work needing to be done to follow developed countries.

6.1.1.3 Policy and Organization Dimension

The aim of this dimension is to find out if digital forensic policies and guidance are popular in Saudi Arabian government organisations. Detailed responses to questions about this dimension are presented in Appendix 3. Nine respondents, including three academic researchers and six practitioners, described that there are no official digital forensic guidelines at present. With no disagreement, every expert said that guidelines are a critical issue within the field of digital forensics. Moreover, all the respondents agreed that there are no regulations or guidelines recommending the third party for digital forensics tool testing in Saudi Arabia. Also, they agreed that the legal enforcement systems do not out-source digital forensic issues. Two experts with different views are both academic researchers, concludes that all digital forensic practitioners agreed that it is not an acceptable way for legal enforcement system to out-source digital forensic issues. These finding findings identify the policy and organization dimension within the field of digital forensics but still leave some gaps need to be clarified more in case interview.

6.1.1.4 Law Dimension

The aim of this dimension is to understand how members of the court consider digital evidence and how the legal enforcement deal with digital forensic issues.

The respondents divided into two groups; one group believes all processes applied to digital evidence should be created and preserved examined by independent third party. While, the other group which include practitioners, think no need to create and preserved examined by independent third party. Unfortunately, the practitioners did not give reasons for their opinion which need to be clarified in the cases interview. Moreover, the respondents agreed that the digital forensic in Saudi Arabia going beyond of existing law. Nine respondents include four academics, and five practitioners believed the reason behind

it is the judges don't have real knowledge about the digital evidence. All the respondents no sure what is required by the court to accept the digital evidence. This indicates there is gap between the courtroom and the legal enforcements involved in digital crimes. However, this is important point to our study need to be clarified more next in case interview

6.1.2 Findings of case study interview

6.1.2.1 Current Situation and Personal Skill Dimension

When we asked the participants what the qualifications are to work as a digital forensic professional, in order to find out the current issues that are associated with certifications of digital forensic experts, practitioners and legal enforcement professionals involved in digital forensics. All participants confirmed that the there are no specific qualifications required to work in digital forensics as far as holding one of the following qualifications: computer science, law, policing and criminology. In order to understand the reasons behind it a lawyer and an investigator were asked direct questions about if nepotism plays a role. Both agree it is quite common not only in the field of digital forensics but almost in every field. Moreover, they stated that the Saudi Arabian government started only eight years ago to give more attention towards digital forensics, to face the fast growth in digital devices related crimes. Also, there is a definite shortage of staff in the digital forensics field, while digital crime grows very quickly in the country.

The experts agree the current situation of digital forensic and digital evidence is critical. There are overlapping tasks between two or more Institutes in their work tasks, which makes people confused. Digital security issues are managed by two different organisations: the Communications and Information Technology Commission and King Abdulaziz City for Science, while digital forensic issues are dealt with by three separate organisations; the Bureau of Investigation and Prosecution, Criminal Evidence Department in Ministry of Interior and Communications and Information Technology Commission. Also, confirm there is no special agent to report cybercrime in Saudi Arabia. Digital crimes can be reported to the Communications and Information Technology Commission,

Regional and local government and police stations. Moreover, two experts added that some people report directly to court especially in case of using digital devices in abusing and insulting. Moreover, there is no particular body in Saudi Arabia to certify the qualifications of digital forensic practitioners and digital forensics institutes/departments. Also, the respondents described that there are no official digital forensic guidelines at present, and there are no regulations or guidelines recommending third parties for digital forensics tool testing in Saudi Arabia.

On the other hand, expert agree that Saudi Arabia does address the importance of information technology in some areas, but still there are huge gaps that exist in the legislation that should be addressed, such as where to report and who should collect and analyze the digital evidence. Moreover, there are different institutes, legislations and regulations that have overlapped each other. Three experts stated it is evident that the practitioners involved in digital forensics needs more training and educations in how to deal with digital evidence and to know what is required by the courtroom to accept it as evidence. Moreover, the judges and lawyers need to have a good knowledge about digital evidence and its strength and weakness.

6.1.2.2 Policy and Organization Dimension

The experts agree that the main challenges faced by digital evidence investigators in Saudi Arabia is how to guarantee the reliability of digital evidence acquired by the court in the absence of national regulations and guidelines. There is an insistent demand from law enforcement professionals and other agencies to validate and verify digital evidence tools to assure the reliability of digital evidence. Also, the experts confirms that the legal enforcement system in Saudi Arabia has been disturbed by introducing digital evidence as a new factor in the legal process and there is huge gap between this new technology and the relevant legislation. An expert describes that government short-term objectives and seniors believes there is no urgent need for new legislation lead to the development of laws cannot keep up with the development of digital forensics. While, another expert added that big companies in Saudi Arabia taking steps forward to develop their own policy and

guidelines to ensure that the organisation is able to secure their system before an e-crime takes place. Also, he confirms that most of the private sector in Saudi Arabia does not have policy and guidelines to detect, collect and identify malicious inside the company system. An expert stated a very important point; he said it is essential in the Islamic law to provide the judge when, where and how the evidence been collected. Therefore, it would be difficult for the courtroom to accept digital evidence in the absence of clear picture how the evidence been collected and analyzed.

When we asked the experts what are laws and institutes in Saudi Arabia deal with technical issues in digital crimes, different answers givens. However, a lawyer explained the law of criminal procedure in Saudi Arabia describes the process of collection of information and evidence necessary for the investigation, and it should be done by a criminal investigation officer and other personnel having powers of criminal investigation without differentiating between classic and modern evidences. This is besides the Anti-cyber Crime law which deals with crimes committed on computers and the E-Transaction Act, which deals with electronic transactions and signatures and provides the guidelines for acceptability of any document or information stored in electronic form. Therefore, there are different organisations dealing with technical issues in digital crimes such as;

1. Ministry of Interior, Department of Criminal Investigation
2. The Bureau of Investigation and Public Prosecution
3. Communications and Information Technology Commission

6.1.2.3 Outcome of Law Dimension

According to the layers the judge's acceptance of digital evidence as a mystique depending on the judge's level of use and understanding of digital equipment. As a result judges do not always make decisions that are consistent with the strength of the laws related to digital evidence. However, the Judges confirm digital evidence could be accepted in the court as Confession (Iqrar) but not as Bayyinah (Clear or strong evidence). Furthermore, he stated it is not a matter of if it is considered equal, lower, or higher than other definitive evidence. It is a matter of how this digital evidence has been collected and how it goes with the crime

scenario. It could be not accepted at all or accepted very ‘low’ or very ‘strong’ but not as Bayyinah. Any crime in the court it is a triangle issue: Judge, Prosecutor, and Respondent. Prophet Mohammed said: “You come to me with your disputes, and perhaps some of you present your cases more eloquently than others. So, if I give a judgment in his favour because of his testimony and because of it, he takes what rightfully belongs to his brother, then I am merely giving him a piece of the fire of Hell, so he should not take it.” The digital evidence still not good enough to be considered as a clear evidence, just like DNA is still not very strong although it is more advanced than digital evidence. Doubt on modern evidence such ad DNA and digital evidence is not only in Saudi Arabia; it is all over the world. I am sure you know about the case of James Simpson where three labs confirmed the DNA but the judges could not use it as good evidence. However, you have to note the in Islamic law there are two methods of proving the crime the first point of view is methods are limited to only specific ways such as witnesses, confession and oath mainly in case of Hudud Offenses. The second point of view is unlimited to include any type of evidence as far as been related to the crime and collected and analysed in scientific and legal way.

On the other hand, the investigators and a lawyer believe that the courts give a low weighting to digital evidence, but it is not clear if it is because of the difficulties in presenting digital evidence in a court or that the members of the court do not understand the concept of digital evidence. Therefore, when we questioned the judge and lawyer, about the important of involving digital forensic specialists in searching, collecting, seizure, investigating, and analyzing digital evidence both agreed it is essential. The second judge confirmed if the digital evidence was not collected in a definite way, then the digital evidence could be vague. Also, he stated as far as I knew, a lot of digital evidence was excluded because the seizure was conducted by non-technical people then forwarded to experts to analyze it where the expert found it unreliable due to miss-use at the first stage.

When we asked the judge what was needed for a courtroom to accept the reliability of testimony related to email, e-signature and e-contract, he stated it is clear in Islamic law that E-contracts or E-signatures are accepted, but the problem lies in proving that transactions have occurred if one party rejects it. Islamic Fiqh Council – Muslim World League, discussed contracts made by modern machines of communication such as computer, fax and/or internet they have decided the contract is legally valid but not in case of marriage contracts as there should be two witnesses.

6.1.2.4 Education and certification Dimension

Experts confirm the result of the survey that the digital forensics is at its early stage and there are limited training institutes and digital forensic specialists to match the rapid growth of digital crimes. Moreover, they agreed that the Saudi Arabian government is recently giving more attention and support towards education and training in the field of digital security and forensics. Furthermore, there is special support from the Ministry of Interior to improve education, training and research in the field of digital forensics. The experts think the situation will change shortly as there are hundreds of students studying abroad in different fields related to digital forensics under King Abdullah high education program. This statement goes with the survey participants; responses that the Saudi Arabian government does realize the importance of digital forensics and it are investing in this field. The survey responses and the findings of the case study interviews and the legal cases shows there is a paramount need for digital forensics programs exist in higher education. An expert stated proper educational programs for the whole legal enforcement practitioners and judges are beneficial for Saudi Arabia to catch-up with the rapid growth of the field of digital forensics.

One of the experts a lawyer stated in Saudi Arabia hardly ever will you find a lawyer having a fair background and knowledge about digital forensics and digital evidence. This is one of the most major issues, there are no specialized lawyers in Saudi Arabia. Most of the lawyers in Saudi Arabia deal with all types of law at the same time such as;

commercial, family, criminal, contracts. Next he was asked so lawyers what do in cases of digital crimes. He stated depends professionalism and faithful but usually search for a computer specialist's to help and advice. However, in most cases the lawyer uses their legal knowledge to defence not the digital forensic knowledge. Oppositely, the major organizations or companies have solicitors with good reputations and international collaborators. The academic added that mostly collection and seizure are carried out by normal non-technical officers in cases of minor individual crimes and could be analysed by technical specialists. While, in cases of crimes with more serious severity issues, like institute hocking, banking fraud, and credit card stealing the Bureau of Investigation and Public Prosecution carry out investigation and the Communication and Information Technology Commission will provide the technical support.

Lawyer and expert investigators believed justice can be achieved only through clear and efficient legal enforcement procedures (investigation and prosecution), trained faithful defence professionals (support for victims) and intelligent and experienced and independent judges. So educating and training judges, about digital forensics alone will not add any value to the legal system in Saudi Arabia in case of digital crimes. This is a new and rapidly growing area of crime, which requires investing in the whole legal enforcement system. This could be done through developing national digital forensic guidelines, training all professionals involved and establishing digital forensics labs following international standards. Further the lawyer stated when we reach such levels, we might need to develop specialized courts for digital forensics where the judges have special training in this field.

6.1.3 Documentary Reports - Legal Cases

Official legal cases are important sources of law, explaining how judges resolved a particular legal dispute and explaining their reasoning. The interpretations of various legal case confirmed the findings of the survey and case interview responses. The legal case (1) showed that law enforcement officers, prosecutors, lawyers, and judges were not aware of the level to which digital information impacts on search and seizure concepts. In addition, these law cases confirm there is no particular body in Saudi Arabia to certify the qualification of digital forensic practitioners and the digital forensic institute/department. Also, there are no official digital forensic guidelines regarding digital forensic issues at present. Moreover, judges do not accept digital evidence in Hudud cases, but they could be accepted in other cases if the judges believe it was collected and presented in legal and scientific methods.

In case one which was taken from the web site of the Ministry of Justice shows that the prosecutor accused the defendant by saying he know him for a long time and in one day he used his mobile phone to make a call, during this period he opened the contacts and copied some names and numbers of the phone. Later on, he used these numbers to insult and abuse the prosecutor by sending messages to those numbers copied from his mobile. The texts were saying that prosecutor is a drug addict, smuggler and homosexual.

Although the case was ten years ago it still shows a number of interesting points related to the study. All calls and text messages done by a mobile phone could be retrieved through the Communications and Information Technology Commission but wasn't done to prove or disapprove the case. Accordingly, the identity of the owner of the mobile could be identified. The mobile could be sent to an expert to investigate it and give his opinion about the issue. However, neither the judge nor the defence lawyer asked to use such methods to approve or disapprove the offence. The judge used the classic methods to approve the offence by asking prosecutor and the witnesses to give the oath. Since he was not convinced enough to apply Hudud punishments eighty lashes for an unproven accusation of being unchaste (Qadhf) the judge used Tazir punishment. Moreover, the

victim reported the incident to the police station and the whole investigation was done at the police station and no digital evidence experts were involved.

In case two Microsoft Saudi Arabia filed a complaint with CITC against Sahara Al-Jazeera, an ISP registered in Saudi Arabia and licensed to provide Internet and Bulk SMS services in the Kingdom of Saudi Arabia by CITC. Microsoft claimed that their SPAM-trap mailboxes captured many SPAM emails sent by Sahara Al-Jazeera on behalf of Giant Stores in the Kingdom of Saudi Arabia. The emails contained a link to the Giant Stores' (Saudi Arabia) website. Sahara sent the messages without the consent of Microsoft and involved the use of a different domain owned by Sahara Al- Jazeerah to send the SPAM messages. The emails did not have an apparent return email address nor an "unsubscribe" option. Microsoft used an international forensics company to trace the originator of the email. The forensics investigation linked the email to Sahara Al-Jazeera, a locally registered ISP in the Kingdom of Saudi Arabia.

The Action Taken: since it was not possible to consider the complaint an offence under any of the existing legislations or regulations, CITC recommended that Sahara Al-Jazeera was made to sign a commitment paper confirming that they would refrain from sending similar messages in the future. In this case there are three important issues raised which are related to this study. Microsoft Saudi Arabia made the complaint that SPAM emails received by Sahara Al-Jazeera direct to Communications and Information Technology Commission (CITC). The second point to note is that Microsoft Saudi Arabia outsourced an international forensics company to trace the originator of the email. The third interesting point is that it was not possible for the CITC to consider the SPAM emails an offence under any of the existing legislation or regulations. While, CITC's report in the same year (2007) showed that 64% of email SPAM received in Saudi Arabia were direct marketing, 25% were sexual emails, 5% were religious emails, and 5% were other types.

In case three filed at CITC by a Saudi Telecom user complaining that he had repeatedly received on his mobile number SMSs containing a link to a local 700 number. The SMSs invited him to participate in a general knowledge competition and win various prizes, including cars and cash. After receiving the invitation a number of times the user decided

to participate by calling the advertised premium rate number. Following some calls to the advertised number, apart from not winning anything, his phone bill reached 5000 riyals, and his line was disconnected.

1. The user registered a complaint with CITC on the grounds that:
2. The Company that sent the messages was not identified in the message.
3. The huge number of messages sent inviting him to participate caused him significant annoyance.
4. The competition probably did not offer any prizes, and instead only sought to make illegal financial gains from the premium rates by making the users repetitively call their 700 numbers.

The action taken CITC decided that they were not able to prosecute the 700 service licensee under the existing laws of the Kingdom, specifically the Telecom Act and its subsequent by laws. CITC decided not to take the case any further, particularly since the company also confirmed that they no longer offer competitions using the 700 service number. This case shows that the existing legislations do not address SPAM in number of aspects, it is obvious that there is significant gaps in the legislative framework which needs to be addressed.

6.2 Discussion

Introduction

Religion influences different cultures in various ways, and it would impact on the culture in various ways at different times. When individuals within a culture believe in a specific religion strongly, the religion will have enormous influence on their culture, where, the culture will accept only those behaviours and ways of thinking that are acceptable to their religion (Aldashev G, 2014). Culture and religion are subjects of modern life in many circumstances, the most important of these are the science, technology, legal issues, politics, industry, commerce, and the various expressive, communicative and creative arts (John Dewey, 1948). Consequently, Saudi Arabian cultural factors have numerous characteristics, which can have strong impacts on the success and security of the society such as language, hierarchy, gender communication, fear of losing face, and favouritism and which may have significant impact on Information communication systems (ICT) (Alkahtani, H, 2013). The standards and framework developed in this study are based on the body of literature reviewed, the findings of the study, ACPO Guideline and IFC recommendation on use of modern evidences. The idea was to generate a simple, easy to understand the standards and framework that contained the specific information needed by an investigator in Islamic countries

The influence of religion and culture in Saudi Arabia as discovered in this study are discussed in more detail in the sections that follow.

Background

The literature, not only illustrates the relationship between religion, culture, and different sciences, but also shows that there is a significant and interesting issue between culture, religion and digital evidence Solano-Flores and Nelson-Barber (2001) stated that, “The conceptual relevance of cultural validity is supported by evidence that culture and

society shape an individual's mind and thinking". Lastly, Greenfield (1997) notes that the way an individual constructs knowledge and creates meaning from experience is affected by culture. On the other hand, Religion influences different cultures in various ways, and it would impact on the culture in various ways at different times. When individuals within a culture believe in a specific religion strongly, the religion will have enormous influence on their culture, where, the culture will accept only those behaviours and ways of thinking that are acceptable to their religion (Aldashev G, 2014). Culture and religion are subjects of modern life in many circumstances, the most important of these are the science, technology, legal issues, politics, industry, commerce, and the various expressive, communicative and creative arts (John Dewey, 1948). Moreover, Maghaireh (2009) stated that the Jordan court system and the judges' knowledge of technological issues (including digital evidence features) is immature, and far from meeting the USA or the Australian level. This is because of the rarity of studies addressing cybercrime issues and lack of opportunity to adjudicate. The Australian and the USA legislatures amended the rules of evidence to include digital evidence. Leidner (2006) reviewed 51 articles which examine cross-cultural studies of Information Technology and established six themes, adoption, diffusion, use, outcomes, management and strategy. These common themes show how different types of firm-wide and cultural values have an impact on information systems development. Furthermore, it shows that the legal enforcement professional's perception of evidence could be affected by some religious and cultural beliefs to the effect that modern evidence cannot be trusted, and traditionalists' views that the law should be based on the traditional religion-based laws. The research issues identified, but not resolved in the literature survey carried out in this study concern the role of digital evidence in legal practice, therefore, the importance of this study is in examining in what way and to what extent Islamic religion and culture affect the status of digital evidence in the legal process? What principles the practitioners have to observe in the way they treat digital evidence in the judicial proceedings? How do digital forensic practitioners resolve the apparent conflict between modern science and Islamic tradition in their daily practice?

The background to this conflict can be found in the Islamic worldview, as presented in

Chapter two above, and is relevant to examination of the role and status of digital evidence, and more precisely, the explanation of its acceptance by the legal and judicial professionals. According to Kamal Hassan (1994), the Islamic worldview is simple and easy to understand. It is based on three fundamental principles which are: TAWHD (theism), KHILAFAH (Vicegerency), and ADALAH (Justice). These principles not only frame the Islamic worldview, but they also constitute the fountainhead of the objectives (Maqasid) and the strategy of Man's life in this world (Hassan, 1994). The Islamic Worldview is a theistic and ethical worldview, which contrasts sharply with the secularist or atheistic alternatives. This worldview emanates from the fundamental belief that life and existence came into being as the result of the will, desire and design of the One and Only Creator (Hassan, 1994). However, Islamic world is not homogeneous regarding religious perspectives; rather it is heterogeneous, consisting typically of traditionalists, and reformists. The fundamental difference between Islamic schools is their understanding and interpretation of the Holy Scripture, and the Prophet's traditions (Parrillo, 2008). In Islamic law there are different types of punishments and different types of evidence accepted in the courtroom depending on the type of crime. Hudud punishments prescribed by God, such as flogging and exiling the unmarried adulterer, stoning the married adulterer, the punishment for highway robbery and flogging the imbiber of liquor. These crimes and their punishments are clearly stated in the Quran, where the judge cannot modify these punishments neither to reduce nor increase them. Moreover, these kinds of punishments can only be carried out on the basis of specific types of evidence such as; confession or the testimony of reliable witnesses since these punishments are God's right. The second type of punishment is retribution (Qisas), where the offender is punished with the same injury that he caused to the victim. Thirdly, the discretionary (Tazir) type of punishment is not fixed by Islamic law, which could be against the rights of God or the rights of a person. It is the broadest category of punishments, where the circumstances and evidence (Qarinah) are used as a method of proving or disproving.

The methods of proving offences in Islamic law are a controversial issue because there are two points of view (AlKarmi 2005; Al-Zohaili 1994). The first point of view

believes that these methods are limited to only classical methods such as witnesses, confession and oath. These views are based on the Quran and the Sunnah (Al-Zohaili 1994). The second point of view is that these methods are unlimited to include any method that leads to the truth such as witness, confession, substantial evidence and a scientific method. Thus, from this viewpoint the Quran allows Muslims to adopt any methods to prove a crime, although the four main Islamic scholars (Hanafi, Maliki, Syafie and Hanbali) acknowledged that it is obligatory for judges to rely on expert evaluations in complex cases (Al-Zohaili 1994).

As the foundations of the Islamic law are in the Islamic religion, legal practice is built on the belief in the relationship between an individual and God, which is moral, ethical and obliges a person to tell the truth in the court of law. Prophet Mohammed said: "You come to me with your disputes, and perhaps some of you present your cases more eloquently than others. So, if I give a judgment in his favour because of his testimony and because of it, he takes what rightfully belongs to his brother, then I am merely giving him a piece of the fire of Hell, so he should not take it." Consequently, there is a conflict between the scientific and impersonal nature of the western legal system that is generated through scientific evidence, and the moral and religious obligation that is based on faith and trust of the Islamic religion. The literature findings confirmed that in Islamic law digital evidence could be accepted in the court as in all types of crimes but not with Hudud offence, since this is offence against God.

The Framework

In this study, participants in the survey and in the case interviews agree that digital evidence would not be accepted in Hudud crimes against God. Furthermore, the legal case (one) where is the offence is under Hudud (sexual slander) the judge does not consider digital evidence and relies only on traditional evidence. Furthermore, in situations when a judge is not certain of the type of offence committed, he would not use Hudud punishments, but would instead use Tazir punishments, Hudud punishments would be harsher than Tazir ones.

Hudud punishments are prescribed by God, and can even include death sentences, such as flogging and exiling the unmarried adulterer, stoning the married adulterer, the punishment for highway robbery and flogging the imbiber of liquor. These crimes and their punishments are clearly stated in the Quran, where the judge cannot modify them, neither to reduce nor increase them. Moreover, these kinds of punishments can only be carried out on the basis of specific types of evidence such as; confession or the testimony of reliable witnesses since these punishments are God's right. Thus it seems that a judge has more discretion in the case of Tazir punishment, and this may be a reason why the harsher Hudud punishments are given only when there is high degree of certainty about the type of crime that was committed.

This is a significant factor that influences the role and status of digital evidence in the SA courts of law. The underlying religious principles directly influence the degree of trust a judge will place upon digital evidence and decisions about what kind of sentencing is appropriate in each given situation. This is in contrast with the western legal practice where judges are more willing to trust in the process and the scientific basis of digital evidence as one distinct form of proof, regardless the type of crimes. In this context, if the evidence is reliable and convincing (because of its scientific basis, rigorous procedure and fit with the legal process) then it is considered as an acceptable form of evidence alongside any other form of evidence (including traditional forms such as witness statements and confessions).

There are two other type of law and punishment in Islamic law that are considered less serious than Hudud and consequently digital evidence would in principle be acceptable; Retribution (Qisas), where the offender is punished with the same injury that he caused to the victim. The other type, the Discretionary (Tazir) type of punishment is not fixed by Islamic law, which could be against the rights of God or the rights of a person. It is the broadest category of punishments, where the circumstances and evidence (Qarinah) are used as a method of proving or disproving guilt.

Literature and research finding confirm there is a doubt about modern evidence,

such digital evidence and it is one of the major issues in Islamic law. Although, the Islamic Fiqh Academy (which is the main Islamic international body of Muslim scholars and experts on subjects of both religious and secular knowledge which promotes the interpretational reflection (ijtihad) of Islamic jurisprudence), agree on using modern evidence in such e-contract and DNA in Islamic law with specific recommendation and guidelines. Interestingly, one of the judges interviewed stated the doubt about modern evidence not limited to Islamic law but worldwide. He gives an example of James Simpson case where the DNA evidence rejected by the court although it was tested and approved by three official labs due to uncertainty. Moreover, when the judge asked what was needed for a courtroom to accept the reliability of testimony related digital evidence such as; email, e-signature and e-contract, he stated Islamic law could accept digital evidence, and this is been discussed by the Islamic Fiqh Council – Muslim World League, discussed contracts made by modern machines of communication such as computer, fax and/or internet and they have decided the contract is legally valid but not in case of marriage contracts as there should be two witnesses. Moreover, the Islamic Law Complex of the Islamic World Organization has decreed that: "…there is no legal objection to using modern, technological advances in criminal investigations and in considering it as evidence in the crimes that do not obligate the court to carry out a prescribed punishment". This can be gleaned from the Sunna, "Avoid prescribed penalties when there are doubts" (Nizar al-Shuayb, 2012). Moreover, the Saudi legal system gives the judges to decide on the evidence and punishment as far as it is note Hudud offences. The judge in such cases is free to use modern methods for producing evidence against the offender. However, depending on the strength of the modern methods used to prove the evidence, the judge may apply a lesser discretionary punishment (Ansary, A. 2015).

However, the judges when they were asked which type of evidence could be considered higher physical or digital evidence, he answered it is not a matter of which is considered lower, or higher the more important one has been collected right and how it goes with the crime scenario. Similarly, when the judges and lawyers, questioned in the case interview about the importance of involving digital forensic expert in searching,

collecting, seizure, investigating, and analysing digital evidence. All agreed if the digital evidence was not collected by trusted, faithful and expert investigators, then the digital evidence could be vague. Also, the judge stated a lot of digital evidence and physical evidence were excluded because the collection, seizure and analyse were conducted by non-technical experts. These finding mean that all judges are traditionalists always reject anything new blindly; instead it could be they question the new type of evidence and seek to find proof that this evidence is as reliable as the more traditional evidence. The findings show that judges do not trust the expertise or the good practices of digital forensic practitioners and therefore do not trust the digital evidence they produce. The solution to the problem seems to be to provide stricter regulations and laws to make the process of discovery, preparation and presentation more 'trustworthy' and to educate the digital forensic experts and to establish stricter professional standards. If these steps were taken then judges would trust the digital forensic experts more and therefore would find their evidence more acceptable. It appear that the judges in Saudi Arabia more likely put their trust in human witnesses (including experts in digital forensics), rather than the scientific process to guarantee the authenticity of digital evidence, due to the prevalent traditionalist views that characterise the Saudi Arabia culture. Unlike, in the west, there seems to be a different emphasis on the trustworthiness of the process (rather than people - i.e. experts). This means that the process itself can be visible, tractable to be checked and investigated if there are any doubts about the authenticity of the evidence. There have also been suggestions that judges themselves could be trained and educated in digital forensic matters - if they understand how the technology works, they will have a better insight into the authenticity of the digital evidence presented to them. Consequently, there is a conflict between the scientific and impersonal nature of the western legal system that is generated through scientific evidence, and the moral and religious obligation that is based on faith and trust of the Islamic religion. Therefore, this difference need to be further researched since the concepts of trust, reliability and authenticity require studies that address the individual dimension in more detail, that investigate other countries and societies (some with less respect for tradition than Saudi Arabia).

Moreover, Saudi Arabia is a newly developed nation with economics which have developed very quickly in a short amount of time with its oil resources. This rapid expansion has shown that there are very limited ICT systems and security experts in Saudi Arabia (ENLASO, 2011). The survey and case interview results shows that Saudi Arabian government started only eight years ago to give more attention towards digital forensics, to face the fast growth in digital devices related crimes. Consequently, there are overlapping tasks between two or more Institutes in their work tasks, which makes professionals confused on their duty. Moreover, digital crimes can be reported to different places the Communications and Information Technology Commission, Regional and local government and police stations. Moreover, two academics added that some people report directly to court especially in case of using digital devices in abusing and insulting. In addition, there is no particular body in Saudi Arabia to certify the qualifications of digital forensic practitioners and digital forensics institutes/departments. These finding shows that repaid growth of digital devices and related crimes in Saudi Arabia has disrupted government.

Experts confirm the result of the survey that the digital forensics is at its early stage and there are limited training institutes and digital forensic specialists to match the rapid growth of digital crimes. Moreover, they agreed that the Saudi Arabian government is recently giving more attention and support towards education and training in the field of digital security and forensics. The survey responses and the findings of the case study interviews and the legal cases shows there is a paramount need for digital forensics programs exist in higher education. An expert stated proper educational programs for the whole legal enforcement practitioners and judges are needed for Saudi Arabia to catch-up with the rapid growth of the field of digital forensics.

One of the experts a lawyer stated in Saudi Arabia hardly ever will you find a lawyer having a fair background and knowledge about digital forensics and digital evidence. This is one of the most major issues, there are no specialized lawyers in Saudi Arabia. Most of the lawyers in Saudi Arabia deal with all types of law at the same time such as;

commercial, family, criminal, contracts. Next he was asked the lawyers what will do in cases of digital crimes? He stated. it depends on his professionalism and faithful but usually will not computer for a specialist's to help and advice. However, major organizations or companies have solicitors with good reputations and international collaborators. According to the academic as a result mostly collection and seizure are carried out by normal non-technical officers in cases of minor individual crimes and could be analysed and defended by un-specialists. Also, he added, in cases of crimes with more serious severity issues, like institute hocking, banking fraud, and credit card stealing the Bureau of Investigation and Public Prosecution carry out investigation and the Communication and Information Technology Commission will provide the technical support.

Lawyer and expert investigators believed justice can be achieved only through efficient legal enforcement procedures (investigation and prosecution), trained faithful defence professionals (support for victims) and intelligent and experienced and independent judges. So educating and training judges, about digital forensics alone will not add any value to the legal system in Saudi Arabia in case of digital crimes. This is a new and rapidly growing area of crime, which requires investing in the whole legal enforcement system. This could be done through developing national digital forensic guidelines, training all professionals involved and establishing digital forensics labs following international standards. Further the lawyer stated when we reach such levels, we might need to develop specialized courts for digital forensics where the judges have special training in this field.

It is a common assumption that judges in Saudi Arabia trust traditional evidence more than modern evidence based on technology and science, because they generally belong to the sections of the society that normally hold traditionalist beliefs and are not in favour of change. The findings of this study, however, indicate that a more likely reason for their distrust is because they believe the digital evidence is not collected, prepared and presented to a sufficiently high standard to ensure that the integrity of digital evidence meets strict requirements, both legal and scientific. Thus the judges' distrust pertains to the legal enforcement practitioners and their practices, not to digital evidence per se. Therefore,

there is a clear gap between the courtroom and the legal enforcements professionals involved in digital crimes, due to the absence of regulations, digital forensic guidelines and institutions to certify the qualifications of digital forensic practitioners and digital forensics institutes. In addition, few legal enforcement practitioners have sufficient technical expertise to analyse digital evidence in case preparation, which is due to the Arab culture of nepotism and insufficient training and education in new and emerging disciplines such as digital forensics.

The impact of culture is that judge's trust in digital evidence and legal enforcement practitioners would be improved if the attitude changed through implementing stricter regulations, training and education programs.

This study has thus identified gaps between courtroom and legal enforcement practitioners. The solution to these gaps seems to be to provide stricter regulations and laws to make the process of discovery, preparation and presentation more 'trustworthy', to educate digital forensic experts and to establish stricter professional standards. If these steps were taken then judges would trust the digital forensic experts more and therefore would find their evidence more acceptable.

Study findings are confirmed in the recommendations of Islamic Fiqh Council – Muslim World League Recommendation for the use modern evidence. According to the IFC, Islamic scholars and judges should put more trust in human experts rather than the scientific process to guarantee the authenticity of digital evidence. Therefore, these recommendations when implemented would satisfy the Islamic law requirements to accept digital evidence in courtroom.

Although ACPO guidelines are accepted in principle as the perfect best practice guide for digital investigations in the UK and many another places, in Saudi Arabia they are adapted to the requirements of the Islamic law and culture. The aim of adopting ACPO guideline is to define a clear, step-by-step procedure for the collection of evidence suitable for presentation in a court of law. However, in daily practice, the courts will still regard witness statements as being more reliable and will therefore prefer the digital forensic

experts to be highly qualified expert witnesses, rather.

Chapter Seven
CONCLUSIONS, LIMITATIONS AND FUTURE WORK

7.1 Conclusion

Literature review, not only illustrates the relationship between religion, culture, and different sciences, but also shows that there is a significant and interesting issue between culture, religion and digital evidence. Furthermore, it shows that the legal enforcement professional's perception of evidence could be affected by some religion and culture beliefs that modern evidence cannot be trusted, and traditionalists believe that the law should be based on the religion traditional legal practice. The research issues identified but not resolved in literature survey concern the role of digital evidence in legal practice, therefore, the importance of this study was examining in what way and to what extent do Islamic religion and culture affect the status of digital evidence in the legal process? What principles do the practitioners have to observe in the way they treat digital evidence in the judicial proceedings? How do digital forensic practitioners resolve this apparent conflict in practice?

The findings show that the role and status of digital evidence in the Islamic law practiced in Saudi Arabia depends on several factors specific to Islam, on individual practitioner's level of education in technology subjects relevant to digital forensics, and to some extent on their religious beliefs. In relation to the type of crime as defined in Islam, Saudi courts do not accept digital evidence in Hudud cases as these are crimes against God and can be proven by traditional evidence only (testimony of witnesses, confession of criminals and oaths). However, digital evidence can be accepted in all other types of crimes if it is collected and presented in a legal and scientific manner. These limitations in accepting digital evidence in courts are similar in both Islamic law and the worldwide. However, in Saudi Arabia, legal enforcement professionals' perception of digital evidence is affected by some Islamic scholars' and judges' beliefs that the law should be based primarily on the traditional religious legal practice. It is a common assumption that judges trust traditional evidence more than modern evidence based on technology and science, because they generally belong to the sections of the society that normally hold traditionalist beliefs and are not in favour of change. The findings of this study, however, indicate that a more likely reason for their distrust is because they believe the digital

evidence is not collected, prepared and presented to a sufficiently high standard to ensure that the integrity of digital evidence meets strict requirements, both legal and scientific. Thus the judges' distrust pertains to the legal enforcement practitioners and their practices, not to digital evidence per se. Therefore, there is a clear gap between the courtroom and the legal enforcements professionals involved in digital crimes, due to the absence of regulations, digital forensic guidelines and institutions to certify the qualifications of digital forensic practitioners and digital forensics institutes. In addition, few legal enforcement practitioners have sufficient technical expertise to analyse digital evidence in case preparation, which is due to the Arab culture of nepotism and insufficient training and education in new and emerging disciplines such as digital forensics.

7.2 Limitations

SCOPE

Digital evidence approval, digital forensic and techniques are complicated, involving many issues such as surveillance, undercover operations, interview and interrogation techniques, arrest, detention, crime scene investigation, fingerprinting, and so on. This thesis, however, examines only part of the main challenges associated with the process of digital investigation to identify in what way and to what extent do culture and religion affect the status of digital evidence in the legal process? As such, this researcher will highlight how culture plays a role in the legal process in Saudi Arabia? And how do cultural factors influence the status of digital evidence?

DATA

Manly there were three major limitations:

1. Limited number of professional and expert in the field of digital forensic in Islamic Saudi Arabia
2. Limited sources about digital evidence, and e-crimes in Islamic literature.
3. Inability to generalize this research over a long period of time in other Islamic cultures

7.2 Future work

The thesis not only shows the impact of religion and cultural in digital investigation and the legal enforcement professional attitudes toward digital evidences in Saudi Arabia, but also provide a framework to present a roadmap to achieve justice between people in case of Cybercrime in Islamic countries.

However, there are a number of areas in which this work can be expanded, in both context, field and the cultures analyzed such as:

- Investigate confidentiality and individual privacy in the course of the investigation of cybercrimes in Saudi Arabia.
- Evaluate judges' awareness, knowledge, and perceptions of digital evidence in Saudi Arabia
- Examine in depth the major parts associated with cybercrime investigation by Saudi law enforcement officers such as searches and seizures of digital evidence.
- Examine in depth why DNA fingerprint result trusted in sSaudi Arabia courtroom more than digital evidence?

.

LIST OF REFERENCES

Mohamed El-Guindy, (2012). Cybercrime researcher Challenges in Middle East, 2012
Sehli H (2015), The role of culture in developing the government absorptive capacity of agencies in Saudi Arabia: a conceptual model, University, Melbourne, Australia. http://www.pacis2016.org/Abstract/ALL/505.pdf
Abdus Salam, H. R. Dalafi, Mohamed Hassan (1994).*Renaissance of Sciences in Islamic Countries*, p. 162. World Scientific, ISBN 9971-5-0713-7.
2001, pp. 36-45.
Abdul-Hakim Al-Tahawi, Al-Malik Faisal Wa Al-Alaqat Al-Kharigiyyah Al-Sa'udiyyah (2002). [King Faisal and the Saudi foreign relation] 34 - 54
Abdulrazaq Al-Murjan, (2008). Network Forensic Investigation of Internal Misuse/Crime in Saudi Arabia: A Hacking Case, ADFSL Conference on Digital Forensics, Security and Law
Aborisade Olasunkanmi, (2011).Development in Africa: The Need for a Culture-Sensitive Approach, J Sociology Soc Anth, 2(2): 97-101.
Abuzahrah, Muhammad (1974) Al-Jarimah wa Al-Uqubah Fi Al-Fiqh al-Islami (crime and punishment in Islamic Jurisprudence). Cairo: Dar al-Fikr al-Arabi.
ACPO Good Practice Guide for Digital Evidence, virsion 5, 2011. http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf
Adel Omar Sherif, Generalities on Criminal Procedure under Islamic Shari.a, in CRIMINAL JUSTICE IN ISLAM, 2003

Agarawala, A., & Balakrishnan, R. (2006). Keepin' it real: Pushing the desktop metaphor with physics, piles and the pen. In ACM Conference on Human Factors in Computing Systems (SIGCHI) (pp. 1283-1292). New York, NY: Association for Computing Machinery.

Ahmad, A. (2002). The Forensic Chain of Evidence Model Improving the Process of Evidence Collection in Incident Handling Procedures. Proceedings of the 6th Pacific Asia Conference on Information Systems.

Ahmed H. Dahlan, supra note 4, at 74; AHMAD AL-DAJANI, KHALID BIN ABDUL AZIZ 115 - 119 (2002); AHMAD H. DAHLAN, supra note 1, at 127 (1984)

Al-alama, M. (2004), "Internet Crime in Islam perspective," The Arabian Journal of security studies and training, 18(36): 5-57.

Alan E Brill, Mark Pollitt and Carrier M Whitcomb, (2006), 'The Evolution of Computer Forensic Best Practices: An Update on Programs and Publications' (2006) Journal of Digital Practice 3, 2.

Aldashev, G. (2014), "Voter Turnout and Political Rents", Journal of Public Economic Theory, DOI: 10.1111/jpet.12141

Ali Siddiqui (1997), The Conception of Justice: Western and Islamic, in JUSTICE AND HUMAN RIGHTS IN ISLAMIC LAW 23, 38 (Gerald E. Lampe ed.,

Ali, A. J. and Schaupp, D.L., Value Systems as Predictors of Managerial Decision Styles. International Journal of Manpower, 13: 19-26.,1992

Ali, A. K. (2005). Using the Delphi Technique to Search for Empirical Measures of Local Planning Agency Power. The Qualitative Report, pp. 718-744.

Aliaga, M., & Gunderson, B. (2000). Interactive Statistics. NJ: Saddle River

Aliaga, M., & Gunderson, B. (2000). Interactive Statistics. Saddle River, p3-15

Alkahtani, H., Dawson, R., and Lock, R. (2013). The impact of culture on Saudi Arabian information systems security. In Proceedings of the 21st International Conference on Software Quality Management (SQM 2013) (Georgiadou, E., Ross, M., and Staples, G. Eds.), pp. 201–210, Quality Comes of Age, Southampton, USA.

AlKarmi, A. (2005), The Wisdom Methods of AlSharia Politics, Bit Alafkar, Libnon.

Alminshawi, M. (2003). 'Internet Crimes in the Saudi Society'. Police Science Deparment. Naif Arab University for Security Sciences. Riyadh.

Al-Murjan A, Xynos K, (2008). Network Forensic Investigation of Internal Misuse/Crime in Saudi Arabia: A Hacking Case, ADFSL Conference on Digital Forensics, Security and Law,

Al-Sanad, A. (2004), The Jurisprudence of Electronic Transaction, Dar Alwarrak, Libnon.

Al-Shuaybi N, (2012), DNA Analysis as Court Evidence in Criminal Cases, http://www.central-mosque.com/fiqh/DNA.htm.

Al-Zohaili, M. (1994), The ways of proofing in Al-Sharia Law, Dar Al-Bian, Syria.

Amaratunga, D., and Baldry, D. (2001). Case Study Methodology as a means of Theory

Building: Performance Measurement in Facilities Management Organisations. Work study, pp.95-105.

Amaratunga, D., and Baldry, D. (2001). Case Study Methodology as a means of Theory Building: Performance Measurement in Facilities Management Organisations. Work study, pp.95-105.

Ami-Narth, J.Y., Williams, P.A.H. (2008). Digital Forensics and the Legal System: A Dilemma of our times. Edith Cowan University.

Anderson, R. (2008). Security engineering (2nd ed.). Hoboken, NJ: John Wiley & Sons.

Anderson, T., & Twining, W (1991) Analysis of evidence: How to do things with facts based on Wigmore's Science of Judicial Proof, Evanston, IL, Northwestern University Press.

Ansary, A. (2015). A Brief Overview of the Saudi Arabian Legal System. New York: Hauser Global Law School Program, New York University School of Law.

Anwarullah (2004) Principles of evidence in Islam. A.S. Nordeen, Kuala Lumpur.

Atiyyah, H.S. (1993), Management Development in Arabic Countries: The Challenges of the 1990s. Journal of Management Development, 12: 3-12.

Ball, C. (2008). What judges should know about computer forensics. National Workshop for District Judges II. Retrieved April 6, 2010, from http://www.craigball.com/What_Judges_Computer_Forensics-200807.pdf

Ball, C. (2008). What judges should know about computer forensics. National Workshop for District Judges II. Retrieved April 6, 2014, from http://www.craigball.com/ What_Judges_Computer_Forensics-200807.pdf

Ball, C. (2008). What judges should know about computer forensics. National Workshop for District Judges II. Retrieved June 13, 2011, from http://www.craigball.com/ What_Judges_Computer_Forensics--200807.pdf

Barbara, J. J. (2005). Digital Evidence Accreditation in the Corporate and Business

Environment. Digital Investigation, pp. 137-146.

Baryamureeba V and Tushabe F, (2004), The Enhanced Digital Investigation Process Model, Institute of Computer Science, Makerere University <http://www.forensicfocus.com/enhanced-digital-investigation-model

Baryamureeba, V. and F. Tushabee, (2006). The enhanced digital investigation process model. Asian J. Inform. Technol., 5: 790-794.

Bassiouni C. (1982), The Rights of the Accused Under Islamic Criminal Procedure, in the Islamic criminal justice system 91, 93.

Beckett J, Slay J. (2007). Digital forensics: validation and verification in a dynamic work environment p.266a.

Beebe N.L., Clark J.G., 2004, A Hierarchical, Objectives-Based Framework for the Digital Investigations Process, in Proceedings of DFRWS 2004, Baltimore, Maryland

BEGC 2013. Comprehensive Study on Cybercrime. UNITED NATIONS OFFICE ON DRUGS AND CRIME.

Boddington R, (2008) Validating digital evidence for legal argument, Australin Digital Forensics Conference, http://ro.ecu.edu.au/adf

Brain D Carrier and Joe Grand, (2004), A Hardware-Based Memory Acquisition Procedure for Digital Investigation (2004) Digital Investigation/Forensic and Evidence Research <http://www.digitalevidence.org/papers/tribble-preprint.pd

Brian Carrier, and Eugene H Spafford, (2003) 'Getting Physical with the Digital

Investigation Process' 2 (2) International Journal of Digital Evidence.
Brill, A.E., M. Pollitt, and C.M. Whitcomb, (2006),The Evolution of Computer Forensic Best Practices: An Update on Programs and Publications.Journal of Digital Forensic Practice, 2006. 1(1): p. 2-11.
Brown C (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice International Journal of Cyber Criminology (IJCC) – Publisher & Editor-in-Chief – K. Jaishankar ISSN: 0973-5089 -
Brown, C. L. T. (2010). Computer evidence: Collection and preservation (2nd ed.). Boston, MA: Course Technology.
Burn, J. K., Saxena, B. C., Ma, L., and Cheung, H. K. (1993) "Critical Issues in IS Management in Hong Kong: A Cultural Comparison," Journal of Global Information Management (1:4), pp. 28-37.
Caloyannides, M. A. (2001) Computer forensics and privacy, Norwood, Minnesota, Artech House.
Carrier, B. (2002). Open Source Digital Forensics Tools: The Legal Argument (Research Report). http://www.digital-evidence.org/papers/opensrc_legal.pdf
Carrier, B. and E.H. Spafford, (2002). Getting physical with the digital investigative process. Int. J. Digit. Evid., Fall, 1: 1-20
Carroll O, Brannon S, Song T, (2008), Computer Forensics: Digital Forensic Analysis Methodology, 2008
Casey, E, (2011). Digital Evidence and Computer Crime – Forensic Science, Computers

and the Internet (3rd Ed.), Elsevier, (2011)
Casey, E. (2002). Error, uncertainty, and loss in digital evidence. International Journal of Digital Evidence, 1(2). Retrieved May 5, 2010, from http://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDEC80B5E5B306A85C4.pdf
Casey, E. (2011). Digital evidence and computer crime: Forensics science, computers and the Internet (3rd ed.). Amsterdam, The Netherlands: Elsevier Academic Press.
Casey, E., & Stellatos, G. J. (2008). The impact of full disk encryption on digital forensics. Operating Systems Review, 42(3), 93-98.
Chau, P. Y. K., Cole, M., Massey, A. P., Montoya-Weiss, M., and O'Keefe, R. M. (2002) "Cultural Differences in the Online Behavior of Consumers," Communications of the ACM (45:10), pp. 138-143.
Chissick M and Kelman A, (2000) Electronic Commerce Law and Practice) Sweet& Maxwell p171. http://www.lawgazette.com.sg/2002-7/July02-feature.htm
Chisum, W.J., & Turvey, B. (2000), "Evidence Dynamics: Locard's Exchange Principle & Crime Reconstruction," Journal of Behavioral Profiling, January, Vol. 1, No. 1
Christensen, L. B. (2007). Experimental methodology (10th ed.). Boston, MA: Allyn & Bacon.
CITC, (2007), REVIEW OF CURRENT LEGISLATIONS AND SELECTED LEGAL CASES, Communication and Information Technology Commission, Final Version Report.
Clayton, M. J. (1997). Delphi: A Technique to Harness Expert Opinion for Critical Decision-Making Tasks in Education, Educational Psychology: An International Journal of Experimental Educational Psychology.
Clayton, M. J. (1997). Delphi: A Technique to Harness Expert Opinion for Critical Decision-Making Tasks in Education, Educational Psychology: An International Journal of Experimental Educational Psychology.
Cohen, F. (2006) Challenges to digital forensic evidence. New Haven, Fred Cohen & Associates.
Cohen, F. (2010). Digital forensic evidence examination (2nd ed.). Livermore, CA: ASP

Press.

Creswell, J. W. (1998). Qualitative Inquiry and Research Design. SAGE Publication.

Curry, A., and Kadash, N., Focusing on key elements of TQMEvaluation for sustainability,The TQM Magazine, 14:207-216, 2002

Custer, R. L., Scarcella, J. A., and Stewart, B. R. (1999). The Modified Delphi Technique –A Rotational Modification. Journal of Vocational and Technical Education. Available at: http://scholar.lib.vt.edu/ejournals/JVTE/v15n2/custer.html

Dafiri, S. (2003), In-Depth Studying of the Law on Criminal Procedure in Saudi Arabia, Dar Tibah, Riyadh.

Daniel J. Ryan; Gal Shpantzer (2010) "Legal Aspects of Digital Forensics". http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf.

Dardick G, et al. (2014), Digital Evidence and Forensic Readiness, Report from Dagstuhl Seminar.
http://drops.dagstuhl.de/opus/volltexte/2014/4549/pdf/dagrep_v004_i002_p150_s14092.pdf

De Vos, A.S. 1998. Research at grass roots: A primer for the caring professions. Pretoria:Van Schaik.

Denscombe, M. 2002. *Ground rules for good research: A 10 point guide for social researchers.* Philadelphia: Open University Press.

Denzin, N. K., and Lincoln, Y. S. (1994). Handbook of Qualitative Research. Thousand Oaks, CA: SAGE.

Dezfoli F, Dehghantanha A, (2003), Digital Forensic Trends and Future, International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(2): 48-76 The Society of Digital Information and Wireless Communications.

DMU, http://www.dmu.ac.uk/research/ethics-and-governance/pg-and-research/human-research ethics/technology/human-research-ethics.aspx

Duren, M., and Hosmer, C. (2002). Can Digital Evidence endure the Test of Time? Proceedings of the Second Digital Forensic Research Workshop.

Duryana Mohamed (2013) cases of electronic evidence in malaysian courts: the civil and syariah perspective, Proceeding of the International Conference on Social Science Research, ICSSR 2013

Edwards, K. (2005) Ten things about DNA contamination that lawyers should know. Criminal Law Journal, 29, 71 - 93.

Elguindy M, (2012), Cybercrime Challenges in Middle East. http://www.academia.edu/5022865/Cybercrime_Challenges_in_Middle_East

Elo, S. & Kynagas, H. (2008). The qualitative content analysis process.Journal of Advanced Nursing. 62 (1), p107-115.

ENLASO (2011). Arabic and Bidirectional challenges for translation and software development. White paper, Retrieved, 5th August 2013 from: http://www.enlaso.com/Language_Tech_Center/White_Papers/Arabic_an

d_Bidirectional_Challenges.aspx

Eoghan Casey, (2004), Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (2nd ed) 104.

Eric. N. BERKOW_TZ, (1993). vedigerleri, Marketing, Irwin Series, 4. Edition, 1993, s. 378.

Fafinski, S. and Minassian, N. (2009) UK Cybercrime Report. Available at: <http://www.garlik.com/file/cybercrime_report_attachement>.

Faigman, David L., et al. 2002. Modern Scientific Evidence: The Law and Science of Expert Testimony. 2d ed. St. Paul, Minn.: West Group

First International Workshop on Systematic Approaches to Digital Forensic

Fischer, A.H. and Manstead,A.S.R. (200), The relation between gender and emotions in different cultures. In: Gender and emotion: Social psychological perspectives A. H. Fischer (ed.), Cambridge University Press. pp71 – 94.

Fitch, K., Berstein, S. J., Aguilar, M. D., Burnard, B., Lacalle, J. R., and Lazaro, P. (2001). The Rand/UCLA Appropriateness Method User's Manual. CA: RAND

Flusche, K. J. (2001) Computer forensic case study: Espionage, Part 1 Just finding the file is not enough! Information Security Journal, 10, 1 - 10.

Forch K, (2004). Legal Methods ofusing computer forensic thechiques for computer crime analysis and investgation. http://iacis.org/iis/2004/ThomasForcht.pdf

Ford, J., Ford, L., & D'Amelio, A. (2008). Resistance to Change: The Rest of the Story. Academy of Management Review, 33(2), 362-377. http://dx.doi.org/10.5465/AMR.2008.31193235

Forrester, J., Irwin, B. (2007). A Digital Forensic Investigation Model for Business Organisations. Department of Computer Science. Grahamstown, Rhodes University

Frank e. Vogel (2000). Islamic law and legal system: studies of Saudi Arabia 142 - 143 & 370 - 373

Gary R. Gordon, Chet D. Hosmer, Christine Siedsma, Don Rebovich, (2003), Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime

available at: https://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf

Ge Zhu, Sunanda Sangwan, Ting-Jie Lu, (2010) "A new theoretical framework of technology acceptance and empirical investigation on self-efficacy-based value adoption model", Nankai Business Review International, Vol. 1 Iss: 4, pp.345 - 372

Gercke M, (2012), *Understanding cybercrime: phenomena, challenges and legal response, available online at:http://www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf*

Gercke, (2006) The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International, 141.

Gercke, M. (2012). A Report on Understanding Cyber-crime: A Guide for Developing Countries. Retrieved from www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Graneheim, U. & Lundman, B. (2004). Qualitative content analysis in nursing research: concepts, procedures and measures to achieve trustworthiness. Nurse Education Today. 24 (3), p105-112

Graneheim, U.H., Norberg, A., Jansson, L., (2001). Interaction relating to privacy, identity, autonomy and security. An observational study focusing on a women with dementia and 'behavioural disturbances', and on her care providers. Journal of Advanced Nursing 36 (2), p256–265.

Greenfield, P. M. (1997). Culture as Process: Empirical Methods for Cultural Psychology. In J. W. Berry, Y. Poortinga, & J. Pandey (Eds.), Handbook of Cross-Cultural Psychology: Vol. 1: Theory and Method. (pp. 301- 346). Boston: Allyn

&Bacon.

Guidotti, Tee L., and Susan G. Rose. (2001). Science on the Witness Stand: Evaluating Scientific Evidence in Law, Adjudication, and Policy. Beverly Farms, Mass.: OEM Press.

Guo Y, Slay J, Beckett J, (2009). Validation and verification of computer forensic software toolsd Searching Function, d i g i t a l inves t i ga t i o n 6, S 1 2 – S 2 2

HALL, E.T., (1976). Beyond Culture. New York: Anchor Books/Doubleday.

Hallaq W, (2009), An Introduction to Islamic Law, https://iuristebi.files.wordpress.com/2011/07/an-introduction-to-islamic-law.pdf

Harissi, Y. and Hefny, A. (2013). Using SAP in electronic government: SAP participation in creating a new E-Government in Saudi Arabia (Doctoral dissertation). Retrieved from https://www.missouriwestern.edu/itm/wp-content/uploads/sites/397/2014/06/Using-sap-in-egovernment.

Hasan, H., and Ditsa, G. (1999)"The Impact of Culture on the Adoption of IT: An Interpretive Study," Journal of Global Information Management (7:1), pp. 5-15

Hill, C. E., Loch, K. D., Straub, D., and El-Sheshai, K. (1998) "A Qualitative Assessment of Arab Culture and Information Technology Transfer," Journal of Global Information Management (6:3), pp. 29-38.

Hofstede, G. (1991). *Culture and organizations: software of the mind*. McGraw Hill

Hofstede, G. (2007). Hofstede's Scores. Available at:

http://www.geerthofstede.com/hofstede_dimensions.php

HOFSTEDE, G., (1980). Culture's Consequences: International Differences in Work-related Values. London: Sage Publications

Hofstede, G., and Bond, M. H. (1988). The Confucius Connection: From Cultural Roots to Economic Growth. Organizational Dynamics, pp. 5-21.

Hong. P.Z. (1991). A Thorny Journey - A Study of the Acculturation Process of Some Chinese ELICOS Students in Brisbane, Australia. Griffith University: Brisbane, Australia.

Hosmer, C. (2002). Proving the Integrity of Digital Evidence with Time. International Journal of Digital.

Hughes B. and Cotterell M., (2002), Software Project Management, 3rd Edition, The McGraw-Hill Companies, UK, ISBN: 0 07 709834 X

Husni A, Nasohah Z,(2013). Prevention of Hudood (Fixed punishments) on doubt and dispute over what is considered doubt and what is not. Advances in Natural and Applied Sciences, 7(1): 23-32.

Ifeyinwa Annastasia Mbakogu, (2004). Is There Really a Relationship Between Culture and Development?, Anthropologist, 6(1): 37-43

Insa, F. (2006). The admissibility of electronic evidence in court (A.E.E.C.): Fighting against high-tech crime: Results of a European study. Journal of Digital Forensic Practice, 1(4), 285-289.

Irshad Abdal-Haqq, (2006). Islamic Law: An Overview of Its Origin and Elements, in UNDERSTANDING ISLAMIC LAW 1, 4 (Hisham M. Ramadan ed.

Ivan P. Fellegi, (2010). Survey Methods and Practices, Statistics Canada's National Contact Centre. Available at: http://www.statcan.gc.ca/pub/12-587-x/12-587-x2003001-eng.pdf

JC Smith, (1981). The admissibility of Statements by Computer' Crim LR 390. The Court of Appeal in R v Spiby quoted this statement with approval.

Jeremy R Poch, (2005), Cyber-Crime and the Uphill Battle Faced by the Business World,

availbe at: http://www.uwplatt.edu/csse/CSSE_411%20Papers%20and%20Presentations/CSSE411Spr2005/PochJ%20-%20%20Final%20Paper.doc> at December 2005

Johnson, E.S. 1981. Research methods in criminology and criminal justice. New Jersey: Prentice Hall.

Jones, C.W. (2005). Council of Europe Convention on Cybercrime: Themes and Critiques. *Workshop on the International Dimensions of Cyber Security*, hosted by the Georgia Institute of Technology and Carnegie Mellon University, 6-7 April.

Joubert, C. 2001. Applied law for police officials. 2nd edition. Cape Town: Juta Legal and Academic Publishers

Kamal M.Hassan, (1994). The Islamic World-View' in Towards a Positive Islamic World-View: Malaysian and American Perceptions, ed. Abdul MonirYaacob& Ahmad Faiz Abdul Rahman (Kuala Lumpur: Institute ofIslamicUnderstanding Malaysia, 11-33; Quotation 12.

Kamali, Mohammad Hashim. Principles of Islamic Jurisprudence. Cambridge, UK: Islamic Texts Society, 2003

Kanungo, S., Sadavarti, S., & Srinivas, Y. (2001). Relating IT strategy and organizational culture: an empirical study of public sector units in India. The Journal of Strategic Information Systems, 10(1), 29 57. http://dx.doi.org/10.1016/S0963-8687(01)00038-5.

Kappos, A., & Rivard, S. (2008). A Three-Perspective Model Of Culture, Information Systems, and Their Development and Use. *MIS Quarterly*, *32*(3), 601-634.

Karagiozis, M.F. & Sgaglio, R. 2005. Forensic investigation handbook: An introduction to the collection, preservation, analysis and presentation of evidence. Illionis: Charles C Thomas Publisher

Karl Seger, David Icove, and William Vonstorch, (1995) Computer Crime a Crime Fighter's Handbook 35
Kaspersky Lab (2015, February 16). Carbanak APT: The Great Bank Robbery. Securelist. Retrieved on 26th February 2015, from https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf.
Kerr, (2005). 'Digital Evidence and the New Criminal Procedure' Columbia Law Review Computer Crime and Intellectual Property Section, above n
Kerr, O. S. (2005). Digital evidence and the new criminal procedure. Columbia Law Review, 105(1), 279-318.
Kerr, O. S. (2009). Computer crime law (2nd ed.). St. Paul. MN: Thomson/West.
Kessler, G. C. (2010). Judges' Awareness, Understanding, and Application of Digital Evidence. Thesis - Norwich University. Available from: http://www.garykessler.net/library/kessler_judges&de.pdf [Accessed: 22nd May 2012]
Kettinger, W. J., Lee, C. C., and Lee, S. (1995) "Global Measures of Information Service Quality: A Cross-National Study," Decision Sciences (26:5), pp. 569-588.
Khurshid Ahmad, (1983) ,IslamiNazriyah-e-Hayat, (Karachi University)
Leedy, P.D. & Ormrod, J.E. 2005. Practical research: Planning and design. 8th edition. Ohio: Merrill Prentice Hall.
Leibolt, G. (2010). The Complex World of Corporate Cyber Forensics Investigations. In J. Bayuk (Ed.), CyberForensics (pp. 7-27). New York: Springer Science+Business Media.
Leidner, D. E., & Kayworth, T. (2006). Review: a Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict. *MIS*

Quarterly, *30*(2), 357-399.

Leidner, D. E., and Kayworth, T. 2006. "Review: A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict," MIS Quarterly, (30:2), 357-399.

LIN, Y.-C. 2008. A Study of Computer Forensics from a Cross-Cultural Perspective: Australia and Taiwan. PhD, The University of South Australia.

Lincoln, Y. S., and Guba, E. G. (1985). Naturalistic Inquiry. Beverly Hills, CA: Sage.

Linstone, H. A., and Turoff, M. (1975). The Delphi Method: Techniques and Applications, Addison Wesley Publishing Company.

Linstone, H. A., and Turoff, M. (1975). The Delphi Method: Techniques and Applications, Addison-Wesley Publishing Company.

Linstone, H. A., and Turoff, M. (2002). The Delphi Method: Techniques andApplications. Available at: http://is.njit.edu/pubs/delphibook/.

lippman M, (1989). Islamic Criminal Law and Procedure: Religious Fundamentalism v. Modern Law, 12 B.C. Int'l & Comp. L. Rev. 29. http://lawdigitalcommons.bc.edu/iclr/vol12/iss1/3

Loch, K. D., Straub, D. W., and Kamel, S. (2003) "Diffusing the Internet in the Arab World: The Role of Social Norms and Technological Culturation," IEEE Transactions on Engineering Management (50:1), February, pp. 45-63.

Losavio, M., Adams, J., & Rogers, M. (2006). Gap analysis: Judicial experience and perception of electronic evidence. Journal of Digital Forensic Practice, 1(1), 13-17.

Losavio, M., Wilson, D., & Elmaghraby, A. (2006). Prevalence, use, and evidentiary issues of digital evidence of cellular telephone consumer and small-scale digital devices. Journal of Digital Forensic Practice, 1(4), 291-296

Luftman, J., and McLean, E. R. (2004)"Key Issues for IT Executives," MIS Quarterly Executive (3:2),pp. 89-104.

Lundman, B., & Norberg, A. (1993). The signifi cance of a sense of coherence for subjective health in persons with insulin-dependent diabetes. Journal of Advanced Nursing, 18, 381-386.

Lundman, B., Norberg, A., (1993). Coping strategies in people with Insulin-Dependent Diabetes Mellitus. The Diabetes Educator 19 (3), 198–204.
M. Taylor, J. Haggerty, D. Gresty, and R. Hegarty, (2010) "Digital evidence in cloud computing systems," Computer Law & Security Review, vol. 26, pp. 304-308
Maghaireh A. 2009. Jordanian cybercrime investigations: a comparative analysis of search for and seizure of digital evidence. PhD, University of Wollongong.
Matthew J Stippich and Christopher J Stippich, (2005) 'A Holistic Perspective on the Science of Computer Forensic', Journal of Information Privacy & Security 27
Matthew Lippman, (1989).Islamic Criminal Law and Procedure: Religious Fundamentalism v. Modern Law,1989.
Mbakogu, Ifeyinwa An. (2004) Is There Really a Relationship Between Culture and Development? © Kamla-Raj Anthropologist, 6(1): 37-43.www.krepublishers.com/02-Journals/T-A
McGuire M, Dowling S, (2013). Cyber crime: A review of the evidence (Report),
Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook (2nd ed.). Thousand Oaks, CA: Sage.
Mingers, J. (2001) Combining IS Research Methods: Towards a Pluralist Methodology, Information Systems Research, pp. 240-259.
Mocas S, 2004. Building theoretical underpinnings for digital forensics research. Digital Investigation;1(1):61e8. Available at: http://www.sciencedirect.com/science/article/B7CW4-4BMXXJS-C/2/9154d2932943f309d86f8a748ac40ab3.
Mohamed D, (2013) cases of electronic evidence in malaysian courts: the civil and syariah perspective, Proceeding of the International Conference on Social Science Research, ICSSR 2013
Mukarram A., & Muzaffar H. S. (Eds.). (2005). Encyclopaedia of Islam. New Delhi: Anmol Publications.

N. H. Gregersen et al. (1998), The Sciences of Nature in an Islamic Perspective" in The Concept of Nature in Science & Theology (SSTh 4/1996), pp. 56–62

Nadler, D., and Tushman, M. Strategic Organization Design, Scott

National Culture and Corporate Adoption of IT Infrastructure,"

Newsted, P. R., Chin, W., Ngwenyama, O., and Lee, A. (1997) Resolved: Surveys have

Newsted, P., Huff, S., Munro, M., Schwarz, A. (1998). A Tutorial on Survey Instruments. MISQ Discovery.

Newsted, P., Huff, S., Munro, M., Schwarz, A. (1998). A Tutorial on Survey Instruments. MISQ Discovery.

Nikki Swartz, (2005) 'Canada to Increase Internet Surveillance' 39 (6) Information Management Journal 22.

Nikzad, N. (2013). Arabic Translation: The importance of breaking the language barrier. Retrieved, 5th August 2013 from: http://www.selfgrowth.com/articles/arabic-translation-the-importance-of-breaking-the-languagebarrier

Noblett, M.G., M.M. Pollitt and L.A. Presley, (2000). Recovering and examining computer forensic evidence. Forensic Sci. Commun., 2: 1-8.

NRC, 2009, Strengthening forensic science in the United States: a path forward (free executive summary). https://www.ncjrs.gov/pdffiles1/nij/grants/228091.pdf

Ogunniyi, M. B. (1988). Adapting Western Science to Traditional African Culture. International journal of Science Education.

O'Harrow, Robert. (2006). No Place to Hide. 1st. Free Press pbk. edn. New York: Free Press

Orin Kerr, 2005, 'Digital Evidence and the New Criminal Procedure' (2005) 105 Columbia Law Review 279
Otto, Jan Michiel (2010). Sharia Incorporated: A Comparative Overview of the Legal Systems of Twelve Muslim Countries in Past and Present. pp. 161–162. ISBN 978-90-8728-057-4.
Parrillo, V. N. (Ed). (2008). Encyclopaedia of Social Problems. Thousand Oaks, CA: Sage.
Patton, M. Q. (1990). Qualitative Evaluation and Research Methods (2nd ed.). Newbury Park, CA: Sage Publications, Inc.
Png, I. P. L., Tan, B. C. Y., and Wee, K. L. "Dimensions of
Pollitt, MM. "Report on digital evidence". CiteSeerX: 10.1.1.80.1663
Radhakrishna, G (2008), The Role of Advertising in Promoting Insurance Services: A Conceptual Approach, Marketing of Insurance Services in India, The ICFAI University Press, Hyderabad.
Ragin, C. C. (1989) The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies, Publisher: University of California Press (March 28, 1989)
Ragin, C. C. (1989) The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies, Publisher: University of California Press (March 28, 1989) Ramsland, K. M. (2001). Forensic Science of CSI. Berkley Trade.
Ratcliff D., 2004, Qualitative Research Methods, Internet. Available from: http://www.vanguard.edu/faculty/dratcliff/index.cfm?doc_id=4254. Accessed:09/09/2004
Ravenscroft, A., & McAlister, S. (2006). Digital games and learning in cyberspace: A dialogical approach. *E-Learning*, *3*(1), 37-50.
Richard A. Lankau, et al. (2007), Mutual Feedbacks Maintain Both Genetic and Species Diversity in a Plant Community, Science 317, 1561
RJ Anderson, (1993). Why Cryptosystems Fail", in Proceedings of the 1st ACM Conference on Computer and Communications Security. pp 215 - 227
Rogers, M.K., J. Goldman, R. Mislan, T. Wedge and S. Debrota, 2006. Computer

forensics field triage process model. Proceeding of the Conference on Digital Forensics Security and Law, pp: 27-40.

Rosen, (1981), Equity and Discretion in a Modern Islamic Legal System, 15 L. & SOC'y 217, 227.

Rothstein, B. J., Hedges, R. J., & Wiggins, E. C. (2007). Managing discovery of electronic information: A pocket guide for judges. Washington, DC: Federal Judicial Center.

Rudolph, P. (2005). Crime and punishment in Islamic law. Cambridge University Press.

Sabbagh, S., Arab Women: Between Defiance and Restraint, Olive Branch Press, Northampton, Mass. 1996

Saferstein R (2009). Criminalistics: An Introduction to Forensic Science (11th Edition). ISBN-10: 0133458822

SALEEM, S. 2015. Protecting the Integrity of Digital Evidence and Basic Human Rights During the Process of Digital Forensics. PhD, Stockholm University.

Saudi Ministry of Foreign Affairs, 2015. http://www.mofa.gov.sa/sites/mofaen/Pages/Default.aspx

Sayed Shah Haneef, Forensic Evidence: A Comparative Analysis of the General Position in Common Law and Sharī'ah, Islamic Studies , Vol. 46, No. 2 (2007),

Schatz, B., Mohay, G., and Clark, A. (2006). A Correlation Method for Establishing Provenance of Timestamps in Digital Evidence. Digital Investigation, pp. 98-107.

Schatz, B., Mohay, G., and Clark, A. (2006). A Correlation Method for Establishing Provenance of Timestamps in Digital Evidence. Digital Investigation, pp. 98-107.

Schjølberg, S., & Hubbard, A.M. (2005). Harmonizing National Legal Approaches in Cybercrime, 10 June 2005, *International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity*, Geneva, 28 June-1 July.

Schjølberg, S., & Tingrett, M. (2004). Computer-Related Offences- A Presentation at the Octopus Interface 2002. Conference on the Challenge of Cybercrime, 15-17 September, Council of Europe, Strasbourg, France. Retrieved 18 August 2007, from http://cybercrimelaw.net/documents/Strasbourg.pdf

Schultz, E. E., & Shpantzer, G. (2010). Information security management handbook. In H. F. Tipton & M. K. Nozaki (Eds.), Security (6th ed., pp. 107–125). Boca Raton, FL: CRC Press.

Shabana A, (2014). Islamic Law of Paternity Between Classical Legal Texts and Modern Contexts: From Physiognomy to Dna Analysis, Journal of Islamic Studies (2014) 25 (1): 1-32.

Shah, G. 2002. Investigation of crime and criminals. New Delhi: Anmol Publications Van Rooyen, H.J.N. 2004. The A-Z of investigation: A practical guide for private and corporate investigators. Pretoria: Crime Solve

Slay, J., and Kearney, D. (2000). An Australian Perspective on the Role of the WWW

Soares, A. M., Farhangmehr, M., and Shoham, A. (2007). Hofstede's Dimensions of Culture in International Marketing Studies. Jurnal of Business Research, pp. 277- 284.

Solano-Flores, G., and Nelson-Barber, S. (2001). On the Cultural Validity of Science Assessments. Journal or Research in Science Teaching, pp. 553-573.

Sommer, P. (2012). Digital Evidence, Digital Investigation and E-Disclosure: A Guide to Forensic Readiness, The Information Assurance Advisory Council (IAAC).

Spenceley, C. (2003) Evidentiary treatment of computer-produced material: a reliability based evaluation. Sydney, University of Sydney.

Straub, D., Loch, K., Evaristo, R., Karahanna, E., and Strite, M. (2002). Toward a Theory-Based Measurement of Culture. Journal of Global Information Management, pp. 13-23.

Tan, B. C. Y., Smith, H. J., and Keil, M. “Reporting Bad News
Tavani, Herman T. (2000). "Defining the Boundaries of Computer Crime: Piracy, Break-Ins, and Sabotage in Cyberspace," Computers and Society, Vol. 30, No
Thatcher, J. B., Srite, M., Stepina, L. P., and Liu, Y. (2003)“Culture, Overload and Personal Innovativeness with Information Technology: Extending the Nomological Net,” Journal of Computer Information Systems (44:1), pp. 74-81.
Trumbull C (2006), Islamic Arbitration: A New Path for Interpreting Islamic Legal Contracts, 629 - 630 Vand. L. Rev., 59 Issue 2
Van Buskirk, E., & Liu, V. T. (2006). Digital evidence: Challenging the presumption of reliability. Journal of Digital Forensic Practice, 1(1), 19-26.
Van Rooyen, H.J.N. 2004. The A-Z of investigation: A practical guide for private and corporate investigators. Pretoria: Crime Solve
Volonino, Linda and Stephen R Robinson (2004), Principles and Practice of Information Security .
Walsham, G. (2002). Cross-cultural software production and use: A structurational analysis. *MIS Quarterly*, *26*(4), 359-380. http://dx.doi.org/10.2307/4132313
Walsham, G. (2002). “Cross-Cultural Software Production and Use: A Structurational Analysis,” MIS Quarterly (26:4), December 2002, pp. 359-380.
Wang, S. J. (2007). Measures of Retaining Digital Evidence to Prosecute Computer-Based Cyber-Crimes. Computer Standards & Interfaces, pp. 216-223.
Wang, S.-J. (2007). Measures of Retaining Digital Evidence to Prosecute Computer-Based Cyber-Crimes. Computer Standards & Interfaces , 29 (2), 8.
Weber, Y., & Pliskin, N. (1996). The effects of information systems integration and organizational culture on a firm’s effectiveness. Information & Management, 30(2), 81-90. http://dx.doi.org/10.1016/0378-7206(95)00046-1.
Webster’s Online Dictionary, Definition Sin, Retrieved 2014, from Website: http://www.websters-online.
Wegman, J. (2005). Computer forensics: Admissibility of evidence in criminal cases. Journal of Legal, Ethical and Regulatory Issues, 8(1). http://findarticles.com/p/articles

/mi_m1TOS/is_1-2_8/ai_n25121965/? tag=content;col1

Wertsch, J. V., Del Rio, P., and Alvarez, A. (1995). Sociocultural Studies of Mind. New York: Cambridge University Press.

Whitcomb, C. M. (2002) An historical perspective of digital evidence: A forensic scientist's view. International Journal of Digital Evidence,

Whitman, M. E., AND Mattord, H. J. (2005) Principles of information security, Boston, Massachusetts, Thomson Learning.

Williams K (2004) Can Urban Intensification Contribute to Sustainable Cities? An International Perspective, City Matters, Official Electronic Journal of Urbanicity, UN Habitat Partnership Initiative, www.urbanicity.org, April.

Wilson, (1999) "Models in information behaviour research", Journal of Documentation, Vol. 55 Iss: 3, pp.249 - 270

within Chinese Tertiary computer Science Education. The Asia Pacific Web

Woudenberg, F. (1991). An Evaluation of Delphi. Technological Forecasting and Social Change, pp. 131-150.

Yasinsac A, Erbacher R,. Marks D, Pollitt M, Sommer P, (2003), Computer Forensics Education, http://www.pmsommer.com/CSDS_Paper.pdf

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., & Sommer, P. M. (2003) Computer forensics education. IEEE Security & Privacy, 1, 15 - 23.

Yin, R. K. (1989). Case Study Research: Design and Methods (Rev ed.). Beverly Hills, CA: Sage Publications

Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, 2010. Adopting Hadith Verification Techniques in to Digital Evidence Authentication. Journal of Computer Science 6 (6): 613-618

Zavrsnik, A. (2010). Towards an Overregulated Cyberspace. Masaryk University Journal of Law & Technology, 4(2), 173-190.

Appendix

Appendix A: Questiuner Survey

Survey Findings

To understand the background of the respondents, four general questions were asked about their education, speciality, place of work and number of years of experience. Their educational attainment and the speciality of the respondents were varied; four with master's degrees in computer science, one with a master's degree in criminology, five respondents are academic researchers from different universities holding PhDs and the other three were police officers holding bachelor's degrees.

The next question was examined the number of years of experience the respondents have in the field of digital forensics. Nine experts have less than three years of experience, and four had around five years' experience in the field. This outcome shows that this field is at its early stage in Saudi Arabia. Moreover, the academic researchers made up around half of the respondents, which could be due to academic researchers being more interested in being involved in a research survey than others.

Current Situation and Personal Skill Dimension:

The various types of modern evidence, such as fingerprints, weapons, or blood, are thoroughly examined by courts to assure admissibility; while digital evidence is neither comprehensively addressed by legislation nor fully evaluated by judges. This situation differs a lot from one country to another. For example, hard drives, Internet files, and e-mail are increasingly coming into more frequent use in courts as courtroom evidence in Western countries, whereas in some other countries, its admissibility is yet to be scrutinised.

Methods of proving the offence in Islamic law is a controversial issue because there are two points of view (AlKarmi 2005; Al-Zohaili 1994). The first point of view believes that these methods are limited to only classic methods such as witnesses, confession and oath. These views are based on the Quran and the Sunna (Al-Zohaili 1994). The second point of view believes that these methods are unlimited to include any method that leads to the truth such as witness, confession, substantial evidence, bearing testimony (Al Qarinah) and scientific methods.

The aim of this dimension is to determine the current situation within the field of digital forensics and personal skill, to better our understanding and develop baselines from which further conclusions may be drawn:

1. Conditions, procedures and characteristics of digital forensics

2. Personal Preference and attitudes toward the skills of digital forensics

3. Restrictions and difficulty within the field of digital forensics

The following four questions were designed to grasp general information about the government's perspective toward digital forensics in Saudi Arabia.

Q. Do you have a specialised department for digital forensics? What is the current condition within digital forensics in your country?

Q. How many years has digital forensics existed as a discipline in your country?

Q. Is digital forensics a topical issue in your country?

Q. What is the government's perspective on digital forensic issues in your country? Do you think the emphasis they put on it is currently at an appropriate level?

In reply to question one, seven participants including three academic researchers, two computer scientists and two officers, agreed that there is no well-established organisation for digital forensics in Saudi Arabia. Five of them further stated that there are two different institutes taking care of digital investigations in Saudi Arabia and that they are;

1. The Bureau of Investigation and Public Prosecution

2. Department of Criminal Investigation, Ministry of the Interior.

The above differences in reply are understandable by being aware of the nature of Saudi culture. It is very common in Saudi Arabia that there are conflicts between two or more Institutes in their work tasks, which makes the people confused.

However, all the participants agreed that the Saudi Arabian government does understand the importance of digital forensics, and there are real efforts to improve this important field. The only exception is that academics stated that the Saudi Arabian government does not put enough weight on digital forensic developments. However, the other participants indicated that the development of digital forensics will be improved shortly.

In answer to question 2, respondents stated that they understood that the Saudi Arabian government started to put an emphasis on digital forensics around 5 to 8 years ago. One participant added that people should not expect digital forensics in Saudi Arabia

to be like in Western countries, since digital forensics were obtained at least 20-25 years ago. Respondents agreed digital forensics is not a topical subject in Saudi Arabia in general, but it is an important topic in legal enforcement against terrorism. This situation is very common in the rest of the Arab world. Due to the uniqueness of computer forensics, it is a subject for experts rather than for the general population. The explanation of the above answers is that Saudi Arabian culture is used to following the lead of Western science. Consequently, the Saudi Arabian government has started to give more attention to digital forensics following the fast growth in this field in Western countries.

Questions 5 and 6 were developed to understand the government's perspective toward digital security issues and digital forensic matters:

All participants stated that there are three different organisations: two dealt with digital security issues and digital forensic issues.

Five participants gave more information about these different organisations. The Communications and Information Technology Commission in collaboration with King Abdulaziz City for Science and Technology, deal with digital security, while the Bureau of Investigation and Prosecution and Criminal Evidence Department, General Directorate of Public Security in Ministry of Interior, deal with digital forensics.

Seven participants further indicated that these organisations cooperate with each other, while the other five participants believed there is no good cooperation between these organisations. This phenomenon can be explained by understanding the Saudi Arabian cultural perspective since it allows the overlapping of tasks between two or more Institutes. However, the Saudi Arabian government understands that digital security and digital forensics are two different topics, and it is logical for them to be dealt with by different institutes.

Question 7 was developed to find out if forensic organization in Saudi Arabia has enough manpower to deal efficiently with digital crimes.

All participants stated that there is a clear shortage of staff in the digital forensics field. Three academics stated that this accepted as there are limited numbers of specialist all over the world. Moreover, they stated that conditions would be worse if no immediate action taken, as digital crime grows very quickly.

Education and certification Dimension:

Few legal practitioners have sufficient technical expertise to analyse digital evidence in case preparation: it is difficult for them to present it in simple, comprehensible terms to judges and juries. What may seem a potentially successful case based on a straightforward legal argument can turn an into a needless failure (Yasinsac et al, 2003). The aim of this dimension is to discover if there exist certifications for computer forensic experts, and organisations regarding training and education in the field of digital forensics. Consequently, the following seven questions were asked to participants to test how digital forensic professionals are educated in Saudi Arabia.

Q. What are the qualifications required in your country to work as a digital forensics professional?

All participants stated that the there is no specific qualification required to work in Digital Forensics as far as the following qualifications: computer science, Law, Policing and Criminology. Two academics gave the two explanations behind it, the first one being that the field is at its early stage in Saudi Arabia. Secondly, there is a significant shortage of specialists to cover the rapid growth of digital uses and its associated illegal issues. This critical point was discussed in more detail in the case interview.

Q. How are Digital Forensic professionals employed in your country? Is it by qualification, experience and/or both?

Two-thirds of the participants stated that both qualification and experience are required, while the other one-third reported that only qualifications are needed. Two academics and one practitioner gave more explanation on this point. In teen education there were very limited numbers (if none) taking specialised digital forensics. Forensic investigators with long experience were employed to do this job. However, the situation is changing with time as more qualified students graduate from national and international Universities.

Q. Do you have training programs for digital investigations and forensic analysis in your country?

All participants stated that the Saudi Arabian government is fully supporting education and training in the field of digital security and forensics. Six participants, including two academic researchers and four practitioners, explained that digital forensics is usually studied in Western countries where Saudis attend. Two more participants stated that the Saudi Arabian government is holding many conferences and workshops in digital forensics. These responses indicate that the Saudi Arabian government understands the importance of digital forensics: though the field is not perfect at this stage and there is much work needing to be done to emulate Western countries.

Q. Do you have in your country an institute or a department to certify Digital Forensic practitioners?

Nine participants agreed that there is no particular institute to certify the qualification of digital forensic practitioners. The nine participants consisted of three academic researchers and six digital forensic practitioners. One specialist stated there is no need to have a specific department to certify digital forensic practitioners as far as they have good qualifications in digital forensics. Two participants answered that they didn't know.

Q. Is there an institute or a department prepared to support research, education and training in the field of digital forensics?

All participants agreed there is great support from the Ministry of Interior to improve educational training and research in digital forensics. Furthermore, two participants stated there are already collaborations between the Ministry of Higher Education, Ministry of Interior and International institutes. These answers show that the Saudi Arabian government understands the difficulties in the field of digital forensics and the importance of speeding the process to improve it.

Q. Do you have on-the-job training programs for Digital Forensic investigators?

On-the-job training provides an excellent opportunity for junior digital forensic workers to learn and understand the latest techniques and cases. Therefore, the above question was asked to find out about the conditions in Saudi Arabia. The findings for this question show that eight experts, including three academic researchers, agreed that there is on-the-job training for digital forensic investigators. However, three participants disagreed with this point of view, as they stated there is no well organised on-the-job training for digital forensic investigators. The answers to this question very important, and there is a need to clarify the answers during interview.

Q. Is it required in your country to have specialised training before being involved in digital forensics?

The answer was that there is no standard digital forensic training for experts within this field, and there are no official institutes to certify digital forensic practitioners either. Moreover, instead of a systematic training method, participants described that there are different ways to train digital forensic experts; such as on-the-job training and short national and international courses. Three participants stated they did not take any particular training before they started their current job. On the other hand, two of them said they did

pass a short course before they started their job. This type of answer can be explained by one cultural reason, that Saudi professionals working in governmental departments tend to avoid giving right answers which might be explained incorrectly.

6.2.3 Policy and Organization Dimension:

A forensic report containing opinions based upon comprehensive digital sources is much more likely to convince a courtroom than opinions based on less reliable sources. The decision in Daubert v. Merrell Dow Pharmaceuticals Inc., 509 U.S. 579, 595 (1993) set forth a five-pronged standard for judges to determine whether scientific evidence is admissible in American courts (Garfinkel, 2009). The standard suggested by Daubert applies to any scientific procedure used to prepare or uncover evidence and comprises the following factors:

A. Testing: Hass the scientific method been independently tested?

B. Peer Review: Has the scientific procedure been published and subjected to peer review?

C. Error rate: Is there any known error rate, or potential to know the error rate, associated with the use of the scientific procedure?

D. Standards: Are there any standards and/ or protocols for the execution of the methodology of the scientific method?

E. Acceptance: Does the relevant scientific community accept the scientific method?

Based on the above factors, the importance of policies and guidelines in the field of digital forensics is understood. Therefore, the aim of this dimension is to find out if digital forensic policies and guidance are popular in Saudi Arabian government organisations.

Q. Computer forensic practitioners and scientists are routinely expected to meet specific standards in order to satisfy legal authorities. Do you have national standards for handling and processing digital evidence in your country?

Nine respondents, including three academic researchers and six practitioners, described that there are no official digital forensic guidelines at present. However, there are digital forensic guidelines proposed by the department which is quite general. Conversely, three respondents stated either ‘I don't ‘ (one) or claimed that they are not familiar with this issue. With no disagreement, every expert said that guidelines are a critical issue within the field of digital forensics.

Q. Do you use any international standards or guidelines for handling and processing digital evidence? Such as ACPO or NIJ?

Eleven respondents answered that they do not use either **ACPO or NIJ**. The other two experts stated that they know about these guidelines but officially there are no international standards recommended to be used.

Q. In your country do you have responsible bodies/ organisations (third party) for digital forensics tool testing?

All the respondents agreed that there are no regulations or guidelines recommending third parties for digital forensics tool testing in Saudi Arabia.

Q. Do legal enforcement systems in Saudi Arabia out-source digital forensic problems?

All the respondents agreed that the legal enforcement systems do not out-source digital forensic issues. Two experts with different views who are both academic researchers, concluded that all digital forensic practitioners agreed it is not an acceptable procedure for legal enforcement systems to out-source digital forensic issues. This situation could be caused due to the law varying from country to country.

Law Dimension

According to Joseph Schacht, "Law is still the most important component in the struggle which is being fought in Islam between traditionalism and modernism under the impact of Western Ideas". However, the theory of law in Islam differs from the theory of the Western of law significantly. Methods of proving an offence in Islamic law is a controversial issue because there are two points of view (AlKarmi 2005; Al-Zohaili 1994). The first point of view believes that these methods are limited to only classic methods such as witnesses, confession and oath. These views are based on the Quran and the Sunna (Al-Zohaili 1994). The second point of view believes that these methods are unlimited to include any method that leads to the truth such as witness, confession, substantial evidence, bearing testimony (Al Qarinah) and scientific methods. Therefore, the aim of this dimension is to understand how members of the court consider digital evidence and how they deal with digital forensic issues.

Q. Is it a requirement that an audit trail or another record of all processes applied to digital evidence should be created and preserved by an independent third party?

The respondents divided into two groups; one group including academics believed it is needed as a very important process to validate the evidence, while the other group which included practitioners, thought there was no need for processes to be examined by an independent third party. Unfortunately, the practitioners did not give reasons for their opinions which need to be clarified in the case interviews.

Q. Do you think digital forensics in Saudi Arabia goes in parallel or beyond current law?

All the respondents agreed that digital forensics in Saudi Arabia goes beyond existing law. Nine respondents, including four academics, and five practitioners believed the reason behind it is that judges don't have real in-depth knowledge about digital evidence.

Q. Which of the following digital evidence would be considered in the courtroom as direct evidence (Bayyinah)or circumstantial evidence (Qarinah)?

A. Data generated by the digital device itself through software such as built-in clocks and remote sensors

B. Documents and records produced by the digital device which are copies of data supplied to the digital device by human beings such as log files, the history of website visits, and metadata.

C. Visible and printable evidence, such as e-mails, Word files and digital pictures.

D. Data that combines other digital-generated documentary evidence such as bank statements and cheques

All the respondents agreed that the first two types of evidence (A and B) would be considered as weak or not circumstantial evidence. Two respondents added if these kinds of evidence have linkages or association with the crime-scene then the courtroom could accept it as circumstantial evidence. On the other hand, there were different answers between the respondents in regard the other two types of evidence (C and D). Three respondents answered that they didn't know, and the rest gave different opinions. The first group included three academics, and two practitioners stated that the courtroom might accept it as direct evidence as far it is not related to Hudud offences and has links or associations with the crime-scene. The other group of eight believed that the answer cannot be generalised as it depends on the case, judge and circumstantial conditions of the crime.

These responses show a clear gap between the courtroom and the legal enforcements involved in digital crimes. Also, it is evident that the practitioners involved in digital forensics do not know what is needed for a courtroom to accept digital evidence. However, this important point in our study needs to be clarified more next in the case interviews.

Appendix B: Cases Interview

CASE ONE FORENSIC INVESTIGATOR

Q. In your organisation, how do you recruit new staff and what backgrounds and technical skills do they have?

In our organisation, there are different ways to recruit new staff, either to choose new graduates from computer science backgrounds, Policing, or law backgrounds, through a particular exam. The second way is selecting staff from other Ministries with the above backgrounds, through careful review. The third way is by recommendation from senior staff without an exam.

Does nepotism play a role?

Yes, I think it is quite common not only in the field of digital forensics but almost in every field.

Q. In Saudi Arabia, what institute deals with technical issues in digital evidence? This may include government departments and private companies.

There are two different institutes taking care of digital forensics in Saudi Arabia;

1. The Bureau of Investigation and Public Prosecution
2. Department of Criminal Investigation, Ministry of Interior

Also, there are some other institutes involved, such as the Communication and Information Technology Commission. There are no private companies or institutes in the country which could help in the investigation. This is one of the major issues discussed among lawyers, as there is no third party whom could help to prove or disapprove a case.

Q. Are there specific training methods for new employees working with digital evidence in your organisation?

Now there is quite a lot of on-the-job training for employees working with digital evidence, and the significant on-the-job training is formal courses for new equipment, including computer forensic hardware and software. Usually, employees working with digital evidence are sent overseas to attend a different type of computer forensic courses and/or conferences. Also, the current methods to train new employees are improving and changing very fast. Furthermore, although the training is developing rapidly among employees working with digital evidence; still, we need more training for those working in the legal part including judges and lawyers.

Q. Do you think that your organisation has enough manpower to deal efficiently with digital crimes?

At this time, there are only a few experts working in the field of digital forensics in Saudi Arabia. For sure, it would be impossible to deal with all digital forensic needs for the whole country, with around 30 million people. However, I think things will change very fast as there are hundreds of students abroad under King Abdullah scholarships studying a different field of computer science. As I said, we have a shortage of manpower, but I think the most important things are the type of qualification, good standard procedures, clear regulations, and useful resources allocated specifically for handling digital forensics.

Q. Generally speaking, there are two common resources of receiving digital evidence; they could be collected either by a forensic specialist or by ordinary non-technical people at the time of seizure before analysis. What are the impacts caused by these two different situations? Is there a difference in the acceptability in court?

The Saudi Arabian government recognises the importance of Information Technology as an essential part of improving administration as well as security. Regulations that are specifically aimed at strengthening economic performance and

internal security were adopted, for example; Saudi Telecom Act and the Anti e-Crime Act both play a vital role. The latter one is assigned to investigate e-criminal cases, gather information, including searching for and seizing evidence, and then to hand over the case to the Bureau of Investigation and Public Prosecution (BIPP). The BIPP, which is a part of the judicial system, is one of the main divisions of the judicial authority conducting further investigation, analysing and labelling crimes, and finally standing before the court to seek conviction for offences.

While the existing legislations in Saudi Arabia do address the importance of Information Technology in in some areas, it is clear there still exists a gap in the legislation, and regulations need to be addressed such as where to report and who should collect and analyse the digital evidence. There are different institutes, and legislations related to digital crimes such as; Ministry of Interior, Communication and Information Technology Commission, Ministry of Commerce (MOC) in the context of consumer protection regulations and Saudi Arabian Monetary Agency (SAMA). So, technically, yes there is a big difference if collected by a digital forensic specialist, or where ordinary non-technical individuals conducted the seizure and forwarded for analysis. However, in real case scenarios, I think nobody bothers about it yet.

Q. In Saudi Arabia, do you have Standard Operating Procedures for the identification, collection, or analysis of digital evidence?

I agree about the importance of Standard Operating Procedures for the identification, collection, or analysis of digital evidence. If the corresponding policies or legislation are not definite, the role of digital forensics is vague. For example, the digital forensic analyst has made certain discoveries after examining the digital evidence. However, these discoveries may not be suitable to be presented at a court because the court does not admit the digital evidence. This is because that the government does not have well-defined policies or legislation for the role of digital evidence. Unfortunately, we have no SOP so far, but our organisation is trying to define SOPs which are suitable for the situation in Saudi Arabia. The organisation already has research results from academic researchers, which are helpful for pointing out the correct direction for building SOPs.

Moreover, our organisation is working together with some other educational Institutes and the Ministry of Justice is trying to obtain the relevant SOPs. However, we can do nothing to change this situation, as the government should take the action. I know some academic groups are trying to develop some in-house SOP, but they are below standard to convince the judge.

Q Do you think the people working in legal enforcement need more training in the field of digital evidence?

Yes, as much as we try to improve the quality of digital evidence, we would not be able to convince either judges nor lawyers if they don't have the basic knowledge of IT.

Q. Do you use any international standards or guidelines for handling and processing digital evidence? In your country do you have responsible bodies/ organisations for digital forensics tool testing?

Unfortunately, we don't have any sort of standards or guidelines for handling and processing digital evidence. We just utilised some functions used in International standards such as hashing the evidence.

Q. In Saudi Arabia are there responsible bodies/ organisations for digital forensics tool testing?

Not yet, according to the best of my knowledge. Even private institutions are not attracted by such a field yet. The question should be raised: why? The answer is that no-one knows.

Q. What are the requirements for the courtroom to accept the reliability of testimony related to digital evidence?

Mostly, the result of the lab test handled to court as technical report by the digital forensic department. For example, in the case of text message crime such as; blackmail (extortion), or sexual harassment, the judges fully rely on the reports of the Communication and Information Technology Commission.

Q. What do the judges require to accept the reliability of testimony related to email and e-contract?

Usually, the judge relies on the reports of the forensic department, and he might ask some questions to understand the case, but never takes the investigator as a witness.

Q. Do you have any idea why no private institutions are involved or have been interested in such a new and growing field?

The industry does not enter the field due to the lack of SLA (service level agreement) and also that cybercrime law is in its infancy. Thus, they (private sector) do not take a risk in such a dark area. They do risk management studies, and I think found it too risky as there is no clear law, strategy and standard body/ organisation to test forensic tools (as I mentioned).

Q. Do the courts in Saudi Arabia consider the digital evidence equal, lower, or higher than other classic evidence? Why?

Unfortunately, lower. Due to lack of knowledge they cannot see how such a case has been established. Thus, they assume most cases are inadmissible!

CASE TWO FORENSIC INVESTIGATOR

Q. In your organization, how do you recruit new staff? What backgrounds and technical skills are required?

I am not sure; but most of them they have a certificate of general computer science, Policing, law or Islamic Law. I think they have to have some computer crime course. My background is in Islamic Law and I took a course in Prince Naif Arab University in digital forensic investigation.

Q. In Saudi Arabia, what institute deals with technical issues in digital evidence? This may include government departments and private companies.

Depending on the type of crime, there are two different institutes taking care of digital forensics in Saudi Arabia;

- The Bureau of Investigation and Public Prosecution
- Department of Criminal investigation, Ministry of interior

Q. What is the most common e-crime reported in Saudi Arabia?

First let me tell you the source of complaints:

1. Reported by the government organization …. Not common, and most commonly related to politics or religion abuse and extortion (either web hacking or terrorism).

2. Reported by the non-government organization …. Not common such as finance (hacking, theft)

3. Reported by the people …. These is the most common which are about abuse and extortion (offense of obtaining money, property, or services or sex from a person, entity, or institution, through coercion). The most common example is men against

women: using her photo or SMS or chatting either with hem (as X-friend) or with another man. Some time women use it as well to get money from the man.

Q. Where do people report digital crimes? Do you have a special agent?

No we don't have a special agent; they can report it to a police officer.

Q. Could you tell me what are the steps taken when reporting such crimes?

1. People go to the police station to make a report about the crime, if it is related to the third type a police officer will write a report about what he sees in the mobile (if it is through SMS or social media the officer report the context and time and date) and if there are photos then the mobile will be taken and sent to the forensics department. If it is related to computer crime or the other two types it will be referred to the Department of Criminal Investigation, Ministry of Interior.
2. The police send all the documents to the Criminal Investigation department in Ministry of Interior. They search for the accused person and fill a special form by investigators for the e-crime.
3. The accused person is then sent to the Bureau of Investigation and Public Prosecution for further investigation. Usually this organization has specialized investigators in all areas of crime such as digital crime.
4. All documents and a full report on the digital evidence (if any) will be send to court.

Q. Are there specific training methods for those working in the police about taking care of complaints?

As far as I know there is no special training for those police officers taking complaints.

Q. Are there specific training methods for those working with digital evidence and for the new employees in your organization?

Yes, there is quite a lot of on-the-job training for employees working in the lab with digital evidence, but still we need more training to those jobs in the police offices where reporting starts.

Q. Do you think that your organization has enough manpower to deal efficiently with digital crimes?

No, Saudi Arabia is a very big country with a big population, and there are only very few digital forensic centres in big cities with few experts. However, I think in a few years things will change very quickly as there are many postgraduates abroad now.

Q. Generally speaking, there are two common resources of receiving digital evidence; either collected by a digital forensic specialist, or where the seizure is conducted by normal non-technical individuals and forwarded for analysis. What are the impacts caused by these two different situations? Is there a difference in the acceptability in court?

As I said earlier, reporting starts from general police officers if it is coming from non-government or from a person, they will be handed to a to specialized department either in The Bureau of Investigation and Public Prosecution or the Department of Criminal investigation, Ministry of Interior. So the seizure is done by normal non-technical individuals and forwarded for analysis. But if it is related to terrorism, it would be handled from the beginning to a specialized department at the Ministry of Interior with a group of officers, some of them digital forensic specialists.

Q. In Saudi Arabia, do you have Standard Operating Procedures for the identification, collection, or analysis of digital evidence?

Unfortunately, not everyone believes in the importance of Standard Operating Procedures, so until now we have not had it yet.

Q. Do you think the people working in law need more training?

Yes, I think all people involved in digital crimes such as police, investigators, prosecutors, lawyers, and judges should have training at some stage. This will improve the quality of digital investigations and control digital crimes.

Q. Do you use any international standards or guidelines for handling and processing digital evidence? In your country do you have responsible bodies/organizations for digital forensics tool testing?

No, but some teams try to implement some of the international standard functions.

Q. Do you use international standards such as NIJ and ACPO?

As I said earlier, officially we don't use either British or American standards, but mostly we follow the same steps they do.

Q. In Saudi Arabia are there responsible bodies/organizations for digital forensics tool testing?

No, and I don't think that there will be in the near future.

Q. Why there are no responsible bodies?

If the basic things have not been done such as setting good guidelines and policy, I think we need a few years to achieve it.

In order for the courtroom to accept the reliability of testimony related to digital evidence, what is the requirement?

Judges never use it as clear evidence, but they might use it as weak, accepted, or very strong hearsay evidence. Usually, our department writes a report about the case signed by investigators and sent to court. The judge goes through the report and co-related the evidence with the events of the crime scene, and he will decide either to accept it as weak, satisfactory or strong hearsay. I think you should know even DNA is never used as clear evidence in the court. Usually, judges use it as strong hearsay, if co-related with the

events of the crime scene. However, this is not like digital evidence that depends on judge contentment.

Q. So, what do the judges require in order to accept the reliability of testimony related to email and e-contract?

They are all treated as the same, but these (email and e-contract) evidence are usually taken as stronger hearsay

Q. Do you have any idea why no private institutions are involved or have been interested in such a new and growing field?

I don't know.

Q. Do the courts in Saudi Arabia consider digital evidence to be equal, lower, or higher than other classic evidence? Why?

Unfortunately it is considered to be lower, but why… I think try to interview one of the judges and ask him about it to add value to your thesis.

CASE THREE (FORENSIC INVESTIGATOR)

Q. In Saudi Arabia, what institute deals with technical issues in digital evidence?

1. Department of Criminal Investigation, Ministry of Interior
2. Communications and Information Technology Commission

Q. What is the most common e-crime reported in Saudi Arabia?

1. Blackmail
2. Phishing
3. Defamation
4. Information leakage
5. Identity theft

Q. Where do people report these crimes? Do you have a special agent?

1. Communications and Information Technology Commission
2. Regional and local government (Al-Eimarah)

Q. What are the steps taken when reporting such crimes?

1. File a complaint in a regional and local government office
2. Attach the evidence
3. Call the victim for an interview

Q. Are there specific training methods for those working in the police and taking care of complaints?

Yes there are, but in my view there is a lack of hands-on training in digital evidence as this subject is very complicated and challenging.

Q. Are there specific training methods for those working with digital evidence and for the new employees in your organisation?

Recently, there has been good collaboration between a number of national and international Universities, depending on an employer and budget.

Q. Do you think that your organisation has enough manpower to deal efficiently with digital crimes?

No. There is a shortage of subject matter and experts in this unique field.

Q. Generally speaking, there are two common resources of receiving digital evidence; either collected by a digital forensic specialist, or where ordinary non-technical individuals conducted the seizure and forwarded it for analysis. What are the impacts caused by these two different situations? Is there a difference in the acceptability in court?

When inexperienced investigators collect evidence, the digital evidence will be subject to modification. You have to understand the right processes to deal with electronic evidence and how to protect the integrity of such evidence by making a forensics image of a target computer, not to access the original data without strong justifications and keeping the record of all processes.

Q. In Saudi Arabia, do you have Standard Operating Procedures for the identification, collection, or analysis of digital evidence?

No, we do not have them, but some private large organisations have international guidelines as a baseline.

Q. Do you think the people working in law need more training in digital evidence?

Of course, yes they need more training to understand the importance of this field.

Q. In your country do you have responsible bodies/organisations for digital forensics tool testing?

No we don't, but the department do tests routinely.

Q. In Saudi Arabia are there responsible bodies/organisations for digital forensics tool testing?

This type of testing needs highly skilled people to run properly and the government is addressing this issue by sending a number of professionals to study abroad.

Q. In order for the courtroom to accept the reliability of testimony related to digital evidence, what are the requirements?

I am not sure, but I think it depends on how much knowledge the judge has about digital evidence.

Q. So, what do the judges require when accepting the reliability of testimony related to email and e-contract?

The challenge here is how to prove the following:

A) The extent of confidence in the way in which it was created or saved as an electronic record or broadcast.

B) The extent of confidence in the way in which the electronic record was signed.

C) The reliability of the method used in maintaining the integrity of the information contained in the electronic record.

Q. Do the courts in Saudi Arabia consider digital evidence equal, lower, or higher than other classic evidence? Why?

In my view, Saudi Arabia considers digital evidence lower than other traditional evidence as they do not realise the importance of digital evidence.

CASE FOUR (JUDGE)

Q. In Saudi Arabia, what institutes deal with technical issues in digital evidence?

All crimes in Saudi Arabia are investigated by the Bureau of Investigation and Public Prosecution, while the technical investigation is done at forensic labs, in the department of Criminal Investigation, Ministry of the Interior.

Q. Are there specific training methods for judges working with digital cases in your country?

Yes, In Saudi Arabia we have an academy called the Judicial Academy and an Institute of Public Administration which is specialized to give training to judges to enhance their skills, improve their expertise, and update them with the information that they require to work efficiently. Furthermore, the new judiciary system requires all judges working in criminal, labour and commercial courts and courts of appeal circuits to have at least 2-3 months of training to learn more about the new regulations and procedures needed for commercial, labour and criminal laws.

Q. Do you think that all judges in your court can deal efficiently with the digital crimes?

As you may know, the main authority for Saudi Courts is Islamic law (Shariah) and the judge is required to have a high standard of Islamic education and knowledge. He should be capable of understanding the socio-cultural issues, and professional skills that will lead to reasonable, just, and impartial judgments. Also, there are other requirements implemented to ensure the presence of qualified judges in each level of the judiciary such as holding a diploma in System Studies, good experience in teaching Islamic studies and experience fulfilling comparable judicial duties. All these requirements should be able to

provide the judges high standards and knowledge to deal with any legal issue, not only digital crimes. However, in complex cases which might need a scientific evaluation such as DNA fingerprints or digital evidence, the judges can rely on expert knowledge and witnesses.

Q. Is there a specific requirement to be an expert to be accepted as a witness?

Yes, the testimony should be given by at least two adult Muslim males with sanity, legal capacity, honesty, accuracy and integrity.

Q. Generally speaking, there are two common resources of receiving digital evidence; either collected by a digital forensic specialist, or where the seizure is conducted by normal non-technical individuals and forwarded for analysis. What are the impacts caused by these two different situations? Is there a difference in the acceptability in court?

As I mentioned before the judges rely on expert witnesses, who should have the knowledge to weigh the evidence. The expert should advise about the quality of the evidence, reviewing all relevant evidence and issues, and give his opinion and explain the complex issues in a way the judge can fully understand. Expert opinions will help the judge to decide if such evidence is to be included or excluded. However, it is very important that the investigators follow well known scientific methods in collecting digital evidence

Q. Do you think the people working in digital forensics need more training?

I think there are a fair number of experts working in this field in Saudi Arabia who need ongoing training, as this technology is growing very quickly. Also, there is the need to educate and train new specialists to be able to cover the whole country. I wish to see

soon a good practical guideline for such complicated evidence to guide the legal enforcement practitioners, lawyers and judges.

Q. In your country do you have responsible bodies/organizations for digital forensics tool testing?

As far as I know there is no official standing institute to test digital forensics tools, but the judges have the power to call experts to do so if needed. However, I think there is urgent need for such an organization, which could serve the whole region not only Saudi Arabia. My advice to you is to put this point as a recommendation for the government.

Q. What is the value of such processes for digital evidence in the courtroom?

It is a very significant process to give more value for the evidence, which might be interesting for the judge.

Q. So, what do you mean by interesting evidence? What information do judges require in order to establish the reliability of digital evidence such as email and e-contract?

Modern evidence like classic ones could be of interest to the judge only if it goes in line with the facts of the crime scene. Sometimes the court receives a number of different pieces of evidence which are difficult to relate to the crime. Using new technology such as email and e-contracts are good samples of digital evidence but if the defendant refused it then it should be examined by an expert.

Q. Do the courts in Saudi Arabia consider digital evidence equal, lower, or higher than other classic evidence? Why?

In Islamic law the methods of proving crime depend on the type of offenses, for example the evidence in case of Hudud Offenses is limited mainly to witnesses, confession and oath. However, digital evidence could be used to support this evidence. In other offences there are unlimited ways to prove or disapprove offences. However, digital evidence is still not strong enough to be considered as standing evidence by itself, just like

DNA test results cannot be used to criminalize the accused. Unfortunately, digital evidence is still at its early stage in Saudi Arabia, and most of the legal enforcement specialists involved lack the knowledge about digital evidence which make it a real issue.

CASE FIVE (JUDGE)

Q. In Saudi Arabia, what institute deals with technical issues in digital evidence?

Department of Criminal Investigation, Ministry of Interior.

Q. What about the Bureau of Investigation and Public Prosecution? Are they involved or not?

They are involved in the investigation and realisation of the crime but not the technical issues. Technical problems are only done at the lab of Ministry of Interior.

Q. Are there specific training methods for judges working with digital cases in your country?

Yes, there are a few judges who study digital crimes from the Islamic law point of view when they are doing their master's or PhD. However, the judge is not authorised to give judgment from his personal knowledge of the case that he had before the case being presented to him in court. Allah's Messenger (Mohammed) said: "You come to me with your disputes, and perhaps some of you present your cases more eloquently than others. So, if I give a judgment in his favour because of his testimony and because of it he takes what rightfully belongs to his brother, then I am merely giving to him a piece of the fire of Hell, so he should not take it." Binothaimeen (2007). The judges may only use the evidence legally recognised in a court of law, like confession and the testimony of witnesses. For sure, the judge needs to be trained to understand the process of the investigation to be able to judge.

Q. Do you think that all judges in your court can deal efficiently with digital crimes?

As far as they have the right Islamic law knowledge, they should be able to effectively address the digital crimes. Digital crimes are just like any classic crime - the difference is only how to collect and make the valid evidence. It is the duty of the second party to prove his case.

Q. Generally speaking, there are two common resources of receiving digital evidence; either collected by a digital forensic specialist, or where ordinary non-technical individuals conducted the seizure and forwarded it for analysis. What are the impacts caused by these two different situations? Is there a difference in the acceptability in court?

I do agree about the importance of the digital evidence being collect by a digital forensic specialist. If the digital evidence is not gathered in the correct way, then the digital evidence could be vague. As far as I know there was a lot of digital evidence that was excluded because the seizure was conducted by non-technical people then forwarded to an expert to analyse it. The expert finds it unreliable due to misuse at the first stage.

Q. Do you think the people working in digital forensics in Saudi Arabia need more training in this field?

Yes for sure, but it is more important to have clear written codes and regulations for digital collection, investigation and analysis, and reporting to court. Once we have these regulations with good training for those people involved in digital forensics we will be more confident to judge such crimes.

Q. In your country do you have responsible bodies/organisations for digital forensics tool testing?

Unfortunately, we don’t have responsible bodies/organisations for digital forensics tool testing.

Q. What is the value of such processes for digital evidence in the courtroom?

It is important, and it is part of Islamic law as stated by Prophet Mohammed: "Avoid prescribed punishments when there are doubts". Doubts can be prevented by collecting and analysing evidence by an expert and doing testing on the digital forensics tools. Avoiding doubts it is the primary job of the police officers, prosecutors, lawyers and judge.

Q. So, what information do judges require to establish the reliability of testimony related to email and e-contract?

The Islamic Fiqh Council – Muslim World League (Reference (52/3/6), discussed contracts made by the modern machines of communication such as computers, fax and/ or internet and they have decided the following:

1. If a contract is made between two individuals not combined by one place and can or can't see or hear each other, but they can contact each other in writing via telex, fax internet or e-mail, and both parties accept the conditions: in this case the contract legally valid.
2. These rules do not include marriage contracts as there should be two witnesses.
3. With regard to the evidence in the case of the possibility of forgery or fraud or mistake, this should be tested according to general rules of proof.

From this we understand that writing a contract is obligatory in Islam, and writing it could be on paper or any method such as the digital writing nowadays.

Therefore, to be able to accept digital evidence we have to prove three primary goals:

1. Make sure the evidence is coming from the original party not from a different person,
2. Make sure the evidence has not been modified or changed,
3. Private and secure information has not been seen by other parties.

An expert in IT could approve these technical issues and only them. Therefore, the legal effect of the electronic message is considered valid and enforceable like a written document if taken into account in the establishment and adoption of the conditions stipulated in the law.

Q. Do the courts in Saudi Arabia consider digital evidence equal, lower, or higher than other classic evidence? Why?

It is not a matter of if it is considered equal, lower, or higher than other definitive evidence. It is a matter of how this digital evidence has been collected and how it goes with the crime scenario. It could be not accepted at all or accepted very 'low' or very 'strong'. Any crime in the court it is a triangle issue: Judge, Prosecutor, and Respondent. Prophet Mohammed said: "You come to me with your disputes, and perhaps some of you present your cases more eloquently than others. So, if I give a judgment in his favour because of his testimony and because of it, he takes what rightfully belongs to his brother, then I am merely giving him a piece of the fire of Hell, so he should not take it." The digital evidence still not good enough to be considered as a clear evidence, just like DNA is still not very strong although it is more advanced than digital evidence. This is not the case only in Saudi Arabia; it is all over the world. I am sure you know about the case of James Simpson where three labs confirmed the DNA but the judge he could not use it as clear evidence. (I think you should read about it, this will help you understand more about how evidence was taken in court.) However, you have to note the Islamic law methods of proving the crime. In Islamic law it is a controversial issue because there are two points of view. The first point of view is methods are limited to only specific ways such as witnesses, confession and oath mainly in case of Hudud Offenses. The second point of view is unlimited to include direct evidence such as witness, confession, or hearsay such as a scientific methods.

Unfortunately, in the case of Saudi Arabia, the lawyers have a lack of knowledge about digital evidence, and they never consider asking an expert.

So, do you think DNA testing is adamant evidence?

It depend on the cases you cannot give general answer, as a general concept yes, but not un Hudud.

.

LAWYERS INTERVIEW

The roles of the lawyers are very significant in the investigation of electronic crime as their missions require them to follow and understand the progress of the case from the beginning and until the courtroom. Also, they have to provide the judges with the justification to accept or reject the evidence. Therefore, the participation of lawyers in this study is critically important as they can explain better the challenges facing legal enforcement professionals in cybercrimes. Two Lawyers were interviewed, as they will be able to provide us in depth information about the current situation in Saudi Arabia and the challenges they are facing surrounding digital evidence and digital forensics.

6.3.3.1 Case Six (Lawyer)

Q. What laws and institutes in Saudi Arabia deal with technical issues in digital crimes?

The Law of Criminal procedure describes the process of collection of information and evidence necessary for the investigation, and it should be done by a criminal investigation officer and other personnel having powers of criminal investigation. This is besides the Anti-cyber Crime law which deals with crimes committed on computers and the E-Transaction Act, which deals with electronic transactions and signatures and provides the guidelines for acceptability of any document or information stored in electronic form. Therefore, there are different organisations dealing with technical issues in digital crimes such as;

1. Ministry of Interior, Department of Criminal Investigation
2. The Bureau of Investigation and Public Prosecution
3. Communications and Information Technology Commission

Q. What is the most common e-crime reported in Saudi Arabia?

For individuals, the most common digital crimes are related to social media which promote adultery, homosexuality and atheism. On Twitter only last year there were around 25,000 accounts targeting Saudis, and around 4,500 accounts that promoted atheism. Hacking, Cyber Terrorism and Virus Dissemination are the major cybercrimes reported by organizations and government.

Q. Where do people report such crimes? Do you have a special agent?

No there is no specific agent that is well known where people can report such crimes. Usually, individuals report the digital crimes and all other crimes direct to Police officers or the regional and local government. Some other people may prefer to take legal action directly through the court especially in cases related to insults and slander. Organizations and some individuals report such crimes to the Communications and Information Technology Commission, or the Bureau of Investigation and Public Prosecution.

Q. What are the steps taken to report such crimes?

As I mentioned earlier, it depends upon the victims and the type of crimes. Either way it is taken the investigation (if required) will go through a specialized agency such as:

1. Ministry of Interior, Department of Criminal Investigation
2. The Bureau of Investigation and Public Prosecution
3. Communications and Information Technology Commission

Q. What do you mean by "if investigation is required"? Do you mean some digital crimes might be taken to court without pre-investigation?

Yes, the victim might decide to take the case directly to the court, especially in cases related to insults and slander. The judge will ask for the evidence and decide if it needs to be sent to the specialised agent to review and give their opinion about it. On the other hand, the prosecutor may ask the defendant to give the Oath if he denied the case. Usually, as you know no false Oath will be given in a courtroom as people are afraid of God's punishment.

Q. Do the lawyers dealing with digital crimes have any sort of educational background or training related to digital forensics?

Unfortunately, hardly ever will you find a lawyer having a fair background and knowledge about digital forensics and digital evidence. This is one of the most major issues, there are no specialized lawyers in Saudi Arabia. You will find most of the lawyers deal with commercial, family, criminal, contracts … cases at the same time.

Q. How are the staff involved in legal enforcement recruited and what backgrounds and technical skills do they have?

There are different ways to recruit new staff: new graduates from different fields through a set of particular exemptions. The second way is selecting staff from other Ministries with required backgrounds, through careful review. The third way is by recommendation from senior staff without an exam.

Does nepotism play a role?

Yes, I think it is quite common not only in the field of digital forensics but almost in every field.

Q. What do lawyers usually do in cases of digital crime?

It depends, if the lawyer is professional and faithful they will search for a computer specialist's help and advice, but some other lawyers try to defend from a classical way. However, this is the case with most individual cases, but not in major cases where organizations or institutes are attached. Usually, major organizations or companies have solicitors with good reputations and international collaborators.

Q. Do you think the people working in law need more training in digital evidence?

Yes, I think the lawyer regulations should be reviewed and amended so that lawyers are classified according to their qualifications, training and experience. In addition, lawyers should take specialized courses according to their specialization frequently and

continuously and everyone involved in digital crime should be trained and have a certificate to be able to work in this field.

Q. Are there any international standards or guidelines used in Saudi Arabia for handling and processing digital evidence? Do you have responsible bodies/organisations for digital forensics tool testing?

Unfortunately, there are no national guidelines or responsible body for digital forensics tool testing, though this is a well-known factor to achieving justice and validating the evidence.

Q. Who collects seizure and analysis digital evidence in Saudi Arabia? Is it done by a digital forensic specialist or non-technical staff?

Mostly, collection and seizure of digital evidence is carried out by non-technical staff but the analysis is then done by digital forensic specialists.

Q. What are the impacts caused by these two different situations?

Most digital evidence is rejected by the judges or considered as Hearsay, due to the uncertainty of the validity of the evidence. The reasons could be because most judges do not trust the procedure and the way used to collect and seize the digital evidence.

Q. What are the requirements in Saudi Arabia for the judges to accept digital evidence?

Saudi Arabia follows Islamic law where the judges enjoy the freedom to chose, accept and/or reject evidence and no one may interfere in the judicial process by altering decisions or redirecting cases. On the other hand, the judges have no power to change the legal enforcement procedure, but still reject any doubtable evidence due to any reasons.

Q. Do the courts in Saudi Arabia consider digital evidence equal, lower, or higher than other classic evidence? Why?

For sure lower, because of the previous reasons I mentioned.

Q. Do you think judges need to be educated and trained about digital forensics?

I believed justice can be achieved only through clear and efficient legal enforcement procedures (investigation and prosecution), trained faithful defence professionals (support for victims) and intelligent and experienced and independent judges. So educating and training judges about digital forensics alone will not add any value to the legal system in Saudi Arabia in case of digital crimes. This is a new and rapidly growing area of crime, which requires investing in the whole legal enforcement system. This could be done through developing national digital forensic guidelines, training all professionals involved and establishing digital forensics labs following international standards. When we reach such levels, we might need to develop specialized courts for digital forensics where the judges have special training in this field.

CASE SEVEN (LAWYER)

Q. In Saudi Arabia, what institute deals with technical issues in digital crimes? This may include government departments and private companies.

There are three of administrative agencies that deal with digital crime:

1. The Bureau of Investigation and Public Prosecution
2. Department of Criminal Investigation, Ministry of Interior
3. Communications and Information Technology Commission

Q. What is the most common e-crime reported in Saudi Arabia?

Cyber stalking, hacking, cyber pornography, cyber terrorism and virus dissemination.

Q. Where do people report these crimes? Do you have a special agent?

Usually, people start by reporting to the police station or the regional and local government. From there either it is referred directly to the court or sent to the Communications and Information Technology Commission, The Bureau of Investigation and Public Prosecution or Department of Criminal Investigation, Ministry of Interior before handled to court.

Q. In which baseline referred to these agents?

Depend on the type of crime and where the victim reports his case all these agents accept reporting digital crimes

Q. What are the steps taken when reporting such crimes?

1. Report the case to the local agent,

2. Case investigated and written report about the content of the digital equipment,
3. If it is related to network or computer will be sent either to the Bureau of Investigation and Public Prosecution or Department of Criminal Investigation, Ministry of the interior before handed to the court.

Q. Are there specific training methods for those working in the police and taking care of complaints?

No, and this is one of the biggest problems in such crimes.

Are there specific training methods for those working with digital evidence and for the new employees in your organisation?

I think so.

Q. Usually, digital evidence is either collected by a digital forensic specialist, or normal non-technical individuals conduct the seizure and forwarded for analysis. What are the impacts caused by these two different situations? Is there a difference in the acceptability in court?

This is the primary reason why the digital is accepted or rejected by the court. If the evidence is not collected in the right way, the evidence would be useless.

Q. In Saudi Arabia, do you have Standard Operating Procedures for the identification, collection, or analysis of digital evidence?

No.

Q. Do you think the people working in law need more training in digital evidence?

Everyone involved in the investigation of a digital crime should be trained and have a certificate for this.

Q. Do you use any international standards or guidelines for handling and processing digital evidence? In your country do you have responsible bodies/ organisations for digital forensics tool testing?

No.

Q. In Saudi Arabia are there responsible bodies/organisations for digital forensics tool testing?

Unfortunately, no such agency exists.

Q. In order for the courtroom to accept the reliability of testimony related to digital evidence, what are the requirements?

It is very easy; all that is required is a clear procedure in collecting evidence done by an expert in the field.

Q. Do the courts in Saudi Arabia consider digital evidence equal, lower, or higher than other classic evidence? Why?

It depends on the type of offence, if the Hudud offence will be considered as supporting evidence. With any other crime, digital evidence could be treated equally with classic evidence.

CASE (ACADEMIC)

Academics working in digital forensic teaching and research usually have advanced knowledge of the digital forensics tools needed to launch a comprehensive and strong digital forensics investigation in civil, criminal, or administrative cases. Also, they are competent to train legal enforcement professionals to carry a complete digital crime scene investigation and have knowledge and skills about the recovery of digital evidence, carrying analysis, presenting a report, and being an expert witness in a courtroom. Therefore, it was necessary to invite academics to participate in this study, as their knowledge about digital crime investigation in Saudi Arabia will add value.

6.3.5.1 Case Eight (Academic)

Q. What is the most common e-crime reported in Saudi Arabia?

We are part of the world so I think we are having the same kinds of cybercrimes types in the rest of the world. However, cyber stalking, hacking, cyber pornography, cyber terrorism and virus dissemination.

Q. In case of cybercrime to whom does the victim first report?

There are different institutes involved in digital crimes in Saudi Arabia. Individual victims start reporting to a police station or the regional and local government. Organizations either governmental or private report to the investigation and the Communication and Information Technology Commission.

Q. Who is doing the investigations and carrying out the technology procedures?

The Bureau of Investigation and Public Prosecution carry out the investigation and the Saudi Arabian Computer Emergency Response Team (CERT-SA) which is a division of Communication and Information Technology Commission or Criminal Evidence Department in Ministry of Interior.

Q. Are digital evidence collection, seizure and analysis done by a digital forensic specialist or by normal non-technical individuals?

Mostly, collection and seizure is carried out by normal non-technical officers in cases of minor individual crimes and analysis done only by technical specialists. In cases of crimes with more severity, like institute hocking, banking fraud, and credit card stealing the Bureau of Investigation and Public Prosecution carry out investigation and the Communication and Information Technology Commission will provide the technical support.

Q. How does the method of collecting digital evidence influence its acceptability in court?

When it comes to collecting and submitting evidence for use in legal processes, the level of care should be applied to the same level in both digital and non-digital evidence. In order for digital evidence to be accepted by the judges, a number of criteria should be met. These criteria and techniques can be met only if the whole process of investigation is done by trained specialized digital forensic practitioners.

Q. Do you think the organizations involved in digital investigations have enough manpower to effectively deal with the digital forensic needs of the jurisdiction of Saudi Arabia?

As an academic, I believe there is not enough manpower to effectively deal with digital forensics in the whole chain of legal enforcement sections. Nether the investigation department, lawyers, nor courts have enough specialized manpower.

Q. Are there specific training methods for new employees working with digital evidence?

Digital forensics in Saudi Arabia needs an urgent move forward to improve through education, training and research. Also, there is a need to encourage graduates from law, computer science and police schools to study digital forensics in higher education.

.

Q. Do you have in Saudi Arabia a national or international standard or guideline for handling and processing digital evidence?

Unfortunately, there are neither national nor international standards/ guidelines for handling and processing digital evidence being used. I think there is an urgent need for the legal system (Shariah Law) in Saudi Arabia to address the challenges and establish national guidelines and establish advanced laboratories for digital forensics. Also, there is a need to encourage Universities to give more intention to invest in research in joint ventures with private sectors.

Q. Do you have in Saudi Arabia responsible organizations for digital forensics tool testing?

This is a very important point, as an academic we believe such independent institutes are needed as a matter of urgency. This will help prove or disapprove the evidence in the courtroom.

Q. What issues do judges in Saudi Arabia face when deciding on admissibility issues related to digital evidence? To what standard of authentication do judges hold digital forensic evidence compared to traditional physical forensic evidence?

Usually, judges place a high weight on classical evidence, but in the case of digital evidence judges give priority to expert testimony that can confirm the authenticity of the evidence. The judges raise several questions such as; what procedures were used during the collection, seizure and analysis of digital evidence to ensure the authentication in procedures? Moreover, asking about the expert's background, sanity, legal capacity, honesty, accuracy and integrity.

APPENDIX C: DECOMENTRY REPORTS (LEGAL CASES)

CASE NUMBER ONE (REF. Q/21/105 - DATE: 17/3/1426 - 26 APRIL 2005)

On Saturday 10/1/1426 at Mohammed Bin Suliman Alseaid the Judge Riyadh Court in the presence of:

The Lawyer MR. XXX the Saudi I.D number: XXX the Prosecution behalf of MR. XXX and the Lawyer Mr. YYY the Saudi ID Number: YYY the Accused behalf of MR.

The Prosecutor stated that MR YYY he knows my client for a long time and in one day he used my client's mobile phone to make a call, during this period he opened the contacts and copied some names and numbers of the phone. Later on, he used these numbers to insult and abuse my client by sending messages to those numbers copied from my client's mobile. The texts were saying that my client Mr XXX is a drug addict, smuggler and homosexual.

Therefore, I request your Majesty to punish him as he did slander my client.

Mr YYY did not accept it, and he said all what has been said is not right, my client was studying in the college which is close to Mr XXX car rental office, and he used to come to the office so frequently to rent a car with his friends. This was the only relation between them, and all the story about the text messages is a lie.

We asked Mr XXX if he had any pieces of evidence about what he said, and the judge said it should be given next time.

On Sunday 25/1/1426 both parties presented to the court, and Mr XXX brought with him a gentleman VVV as a witness. He stated I am a police officer working at the police station (Alswaidy Station) I received an order from my director to go with two colleagues from another police station (Aldeara Station) in the presence of Mr XXX who reported the offence. As soon as we reached Mr YYY's office, we called the mobile number sending the

abusing text while we were looking at him from behind the window. As soon as his mobile rang he answered then he closed it. I repeated it three times and he kept responding. At this stage, I did introduce myself to him as an officer from the police, and I ask him about his ID. He claimed he did not have his ID at this time and when we asked him to go with us to the police station refused and tried to break his mobile but he couldn't. We arrested him, and we saved his mobile phone and his name in the ID was Mr YYYY this is all that I know.

The second witness Mr ZZZ stated the same, as Mr VVV.

Bothe witnesses were asked to give the Oath that all that was said was the truth.

We asked the Accused Mr. YYY, about what the witnesses said. He stated I was in my office suddenly four ordinary men jumped to me and tied me with my scarf on my neck until I lost consciousness until I reached the police station. All I know I did not send these messages and this mobile number does not belong to me.

On Sunday 24/2/1426, both parties presented to the court, and Mr XXX brought with him two gentlemen as a witness. The first one Mr. GGG stated I did receive a number of messages from this mobile number ……. (Place of issue) which were insulting Mr XXX (two text messages) were read from Mr GGG mobile number directly in our presence the judge said.

The second witness Mr. KKK stated I did receive a number of messages from this mobile number ……. (Place of issue) Which were insulting texted messages (three text messages) read from Mr KKK mobile number directly in our presence the judge said.

Both witnesses asked to give the Oath that all that was said was truth.

We asked the Accused Mr. YYY, about what the witnesses said. He stated I did not send these messages and this mobile number does not belong to me.

At the end of this trial, we asked Mr. XXX the Prosecution to bring next time two Identifiers for each witness.

On Sunday 1/3/1426 MR. XXX the Prosecution came with three Identifiers for each witness to give a witness that these witnesses are known to be honest, and sincere.

On Monday 9/3/1426 we reviewed the police report for the contents of the mobile and witnesses sayings. As the two reliable witnesses confirmed, they rang the mobile number ……. (Place of issue) and MR YYY answered, and he tried to break it. Also, the other three honest witnesses confirmed they received a number of the insulting messages from the mobile number ……. (Place of issue).

Therefore, the judgment is as following:

Not to apply the false accusation of illegal sexual intercourse punishment (Hudud Offence), as there is Doubt he sent it from his mobile phone (Place of issue).

Hence, Ta'azir would be applied, with 70 lashes with a whip.

We asked MR. XXX the Prosecution if he accepts the judgment, but he denied the offence and refused the penalty. We informed him he could appeal to the Supreme Court within 30 days.

It was approved by the Supreme Court on 27/4/1426 with reference number: 279/G2/A.

Overview

Although the case wass ten years ago it still shows a number of interesting points related to the study. All calls and text messages done by a mobile phone could be retrieved through the Communications and Information Technology Commission. Accordingly, the identity of the owner of the mobile could be identified. The mobile could be sent to an expert to investigate it and give his opinion about the issue. However, neither the judge nor the defence lawyer asked to use such methods to approve or disapprove the offence. The judge used the classic methods to approve the offence but he was not convinced enough to apply Hudud punishments. Moreover, the victim reported the incident to the police station and the whole investigation was done at the police station.

CASE BY MICROSOFT AGAINST SAHARA (ADOPTED FROM CITC, 2007).

Microsoft Saudi Arabia filed a complaint with CITC against Sahara Al-Jazeera, an ISP registered in Saudi Arabia and licensed to provide Internet and Bulk SMS services in the Kingdom of Saudi Arabia by CITC. Microsoft claimed that their SPAM-trap mailboxes captured many SPAM emails sent by Sahara Al-Jazeera on behalf of Giant Stores in the Kingdom of Saudi Arabia.

The emails contained a link to the Giant Stores' (Saudi Arabia) website. Sahara sent the messages without the consent of Microsoft and involved the use of a different domain owned by Sahara Al- Jazeerah to send the SPAM messages. The emails did not have an apparent return email address nor an "unsubscribe" option. Microsoft used an international forensics company to trace the originator of the email. The forensics investigation linked the email to Sahara Al-Jazeera, a locally registered ISP in the Kingdom of Saudi Arabia. Microsoft then filed a complaint with CITC, through their lawyers in the Kingdom of Saudi Arabia, along with a copy of the forensic investigation report.

The Approach Taken: CITC undertook the investigation of the case. The evidence provided by Microsoft was considered in detail. A representative from Sahara Al-Jazeerah was called in by CITC for questioning. The representative admitted the company's responsibility for sending the emails, which were found to have been sent out in bulk to email addresses obtained using an email harvesting software.

The investigation report, filed by CITC, stated that this case could only be prosecuted under Clause 11- Section 37 of the Telecom Act, by considering it a case of "Misuse of telecom to cause annoyance". However, since the term "annoyances" had not been clearly defined in the Telecom Act and was considered to be ambiguous, it could not be applied to this case. This was particularly so since such emails were sent out only 2-3 times a month.

The Action Taken: since it was not possible to consider the complaint an offence under any of the existing legislations or regulations, CITC recommended that Sahara Al-Jazeera was made to sign a commitment paper confirming that they would refrain from sending similar messages in the future. The CITC legal department sent the report and the related recommendation to the Committee of Arbitration and Dispute Resolution in Telecom related matters. The Committee was requested to revert within a stated period in case they did not agree with the recommendation. Since the Committee did not return with a contradicting decision within the stated notice period, the case was considered closed by the legal department.

Overview

In this case there are three important issues raised which are related to this study. Microsoft Saudi Arabia made the complaint that SPAM emails received by Sahara Al-Jazeera direct to Communications and Information Technology Commission (CITC). The second point to note is that Microsoft Saudi Arabia outsourced an international forensics company to trace the originator of the email. The third interesting point is that it was not possible for the CITC to consider the SPAM emails an offence under any of the existing legislation or regulations. While, CITC's report in the same year (2007) showed that 64% of email SPAM received in Saudi Arabia were direct marketing, 25% were sexual emails, 5% were religious emails, and 5% were other types.

MOBILE SPAM CASE (ADOPTED FROM CITC, 2007)

This case was filed at CITC by a Saudi Telecom user complaining that he had repeatedly received on his mobile number SMSs containing a link to a local 700 number. The SMSs invited him to participate in a general knowledge competition and win various prizes, including cars and cash.

After receiving the invitation a number of times the user decided to participate by calling the advertised premium rate number. Following some calls to the advertised number, apart from not winning anything, his phone bill reached 5000 riyals, and his line was disconnected.

The user registered a complaint with CITC on the grounds that:

1. The Company that sent the messages was not identified in the message.
2. The huge number of messages sent inviting him to participate caused him significant annoyance.
3. The competition probably did not offer any prizes, and instead only sought to make illegal financial gains from the premium rates by making the users repetitively call their 700 numbers.

The Approach Taken: upon receiving the complaints from the user, CITC opened an investigation on the matter and called in the 700 services licensee's representative for questioning. The investigation determined that the promotional SMS messages were being sent from outside Saudi Arabia. When interviewed, the 700 services licensee's representative denied all allegations about sending bulk SMS messages to promote their services, both directly from inside Saudi Arabia, or by hiring a cross-border service provider. He also claimed those messages could be sent by competitors to damage his company's reputation.

The company's representative also stated that his company had been using a provisionally allotted 700 number for the purpose of competitions. However, they had

recently stopped all further competitions using their provisional 700 number, since the formal approval for the 700 number is still pending.

The Action Taken: CITC decided that they were not able to prosecute the 700 service licensee under the existing laws of the Kingdom, specifically the Telecom Act and its subsequent by laws.CITC decided not to take the case any further, particularly since the company also confirmed that they no longer offer competitions using the 700 service number.

APPENDIX D: RECOMMENDATION

Background

These recommendations are based on the body of literature reviewed, the findings of the study, ACPO Guideline and IFC recommendation on use of modern evidences. The idea was to generate a simple, easy to understand the standards and framework that contained the specific information needed by an investigator in Islamic countries.

1. **Thesis finding and outcome**

   The findings of this study identified the gaps between courtroom and legal enforcement practitioners. The solution to these gaps seems to be to provide stricter regulations and laws to make the process of discovery, preparation and presentation more 'trustworthy', to educate digital forensic experts and to establish stricter professional standards. If these steps were taken then judges would trust the digital forensic experts more and therefore would find their evidence more acceptable.

2. **Islamic Fiqh Council – Muslim World League Recommendation for use modern evidence**

   Study findings and the IFC recommendations shows that Islamic scholars and judges put more trust in human experts rather than the scientific process to guarantee the authenticity of digital evidence. Therefore, these recommendations implemented in this framework would satisfy the Islamic law requirements to accept digital evidence in courtroom.

3. **ACPO Guideline**

   This guideline is accepted as the perfect best practice guide for digital investigations in the UK and many another places. The aim of adopting ACPO guideline is to define a clear, step-by-step procedure for the collection of evidence suitable for presentation in a court of law.

Standards for collecting electronic evidence in Islamic countries

Principles

These principles apply to all legal systems using digital evidence to ensure that such evidence is reliable, credible – etc**.)**

1. Digital investigations order should be done either by a judge or authorized officers.
2. Digital investigations should be performed only in digital laboratories with the following conditions:
   a) Certified laboratories from well-organized institute.
   b) The digital laboratories should be equipped with the best and latest technological resources, and should be at of international standard.
   c) The entire tool testing system in the laboratories should be examined routinely by responsible bodies.
3. All digital testing analysis steps should be documented by the investigation team.
4. Digital investigation should be done by two different forensic laboratories.
5. The digital forensic team should be a group at least of three experts; scholars, digital forensic specialist, and officer.
6. The digital forensic team should meet the following conditions: sanity, legal age, legal capacity, honesty, accuracy and integrity. If one condition or more is violated, the test result should not be accepted (Islamic Fiqh Academy guideline for DNA tests).
7. Both parties (the victim and a suspect) have the right to consultation from a private consultant agent to examine the processes of collecting the evidence;
8. The digital forensic team has the overall responsibility for ensuring the privacy of personal information of subscribers.

9. The digital forensic team is required to provide a report to the courtroom

10. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court (ACPO).

11. In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions (ACPO).

12. An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result (ACPO).

13. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to (ACPO).

Digital Forensic gouidlines

The following steps should be followed carefully to ensure the evidence collected is complying with Islamic law:

1. **Initial phase:**
    A. **Guideline**: Policies and procedures in place to assist in the investigation
    B. **Identity of victim**: Reporting identity should confirmed;
    C. **Reporting Place**: Cybercrime should be reported in a special Cybercrime police office
    D. **Reporting officer:** Should be a well-trained officer;
    E. **Documentation**; Document all evidence provided by the victim including name and ID of witnesses (if any);
    F. **Interviewing the victim and collecting related information;** about the devices and operating system, file structure, types of attacks, when it happened, how, and where and the consequences of the attacks (The International Association of Computer Investigative Specialists 2007);
2. **Avoid cronyism:** the identity of the suspect should be kept from the digital forensic

3. **Searching Phase**

The definitive objective of this phase is to search for information that relates to the specific crime and to protect the privacy of people. Actually, searching is very restricted in Islamic law as it might breach the privacy of people. The Qur'an states ***"O you who have believed, avoid much [negative] assumption. Indeed, some assumption is sin. And do not spy or backbite each other. Would one of you like to eat the flesh of his brother when dead? You would detest it. And fear Allah; indeed, Allah is Accepting of repentance and Merciful"***.

A. Physical Examination

1. **Verify the condition** of the digital device: if it is switched off some information might not be recovered. (ACPO guidelines)
2. **Document a**ll physical descriptions (should include all details);
3. **Protect the integrity** if violating the privacy of the offender's digital devices.
4. **Record** in detail all findings.

B. Digital Examination

1. **Directory listing** should include filenames and time stamp.
2. **Log files** should be located and examined.
3. **File viewers** could be used to examine files created by the suspect.
4. **Examining files** in the operating system (such as temporary and history files).
5. **Extract** all evidence.
6. **Automated forensic analysis tools** can be used only if they are at an international standard
7. **Copy and print** only related files and images

4. Seizing phase

The main aim of seizing is to preserve the evidence by legal power to protect the integrity, accessibility and availability of evidence to prove or disprove an accusation.

A. **Record** the time of seizing and all data without accessing the devices
B. **Seize** only the devices used and related evidence and keep them in a safe box
C. **Protect** the privacy of the seized items
D. **Return** all seized devices, papers, images and documents

5. Analysis Phase

The aim of this phase is gathering all available information to build a clear picture about the crime by establishing or disapproving the link between the crime and the suspect. This phase is vital as it will help the judge to make the right decision.

A. **Integrity of the evidence** should be protect by not reexamining original data
B. **Avoid b**ias by not hiding the name of the suspect
C. **The forensic team** is responsible for gathering and analyzing all the available information
D. **Recorded** all processes
E. **Report** the digital forensic team is required to provide the courtroom a report with the following (Garfinkel, 2009):
    a) **Testing:** Has the scientific method been independently tested?
    b) **Peer Review:** Has the scientific procedure been published and subjected to peer-review?
    c) **Error rate:** Is there any known error rate, or potential to know the error rate, associated with the use of the scientific procedure?
    d) **Standards:** Are there any standards and/ or protocols for the execution of the methodology of the scientific method?
    e) **Acceptance:** Does the relevant scientific community accept the scientific method?